

Güvenlik Yönetimi

ÖZEL GÜVENLİK SEKTÖRÜNÜN SESİ ● AYDA BİR YAYINLANIR

HAZİRAN 2026 SAYI: 155

KAPAK:
ULAŞIM
GÜVENLİĞİ

FOKUS:
TÜNEL
UYGULAMALARI

ÖZEL DOSYA:
HEMŞİRE ÇAĞRI
SİSTEMLERİ



**Geleceęi
göremeyiz ama
çözümlerimiz ile
geleceęi
koruyabiliriz**

İhtiyaçlar deęişse de esnek ve adaptif teknolojilerimiz ile her duruma hızlıca uyum sağlıyoruz.

Sunduğumuz teknolojilerle geleceęin güvenliğini şekillendiriyor, dünyanın daha güvenli hale gelmesine yardımcı oluyoruz.

Farklı bir dünya görüyoruz



GÜVENLİKTEDARİK.com

Son teknolojiye uygun, ürün ve çözümlerden **HABERİNİZ VAR MI?**

- Elektrik proje taahhüt firmaları • Bayi odaklı çalışan firmalar
 - Havalimanları ilgili birimleri • Bankalar ilgili birimleri • İnşaat firmaları
 - Oteller ilgili birimleri • Hastaneler ilgili birimleri • AVM'ler ilgili birimleri
 - TÜRKİLM Üyeleri • Belediyeler ilgili birimleri • Emniyet Genel Müdürlüğü ilgili birimleri • Zincir mağazalar • Üniversiteler • Mimarlık ofisleri
 - Sektör profesyonelleri **AĞIMIZA KATILIN**
- ### TÜM TÜRKİYE'DE SESİNİZ OLALIM!

- ✓ CCTV ve video kontrol sistemleri,
- ✓ Yangın algılama ve ihbar sistemleri,
- ✓ Yangın söndürme sistemleri,
- ✓ Geçiş kontrol sistemleri,
- ✓ Hırsız alarm sistemleri,
- ✓ Alarm izleme merkezleri,
- ✓ Apartman konuşma sistemleri,
- ✓ Mobil takip sistemleri,
- ✓ Drone teknolojileri

Çok sayıda MİKE TİMMER çözümlediği resmi ve özelde işletmeleri koruyan bir hizmet ağına olan **ARKHO TANITIM HİZMETLERİ** tarafından hizmet verilmektedir. Başta saade GÜVENLİK YÖNETİMİ, PERFORMANÇ, TEKNİKLER ve KURUMSAL YATIRIMCI dengeleri barındıran **ARKHO TANITIM HİZMETLERİ** grafik tasarım, kurumsal kimlik çözümleri, web ve farklı dijital promasyon araçları ile çok yönlü hizmetler, her ve müşteriye koruyucu bir politikaya göre çözümler sunmaktadır.

Güvenlik Yönetimi
ARKHO TANITIM HİZMETLERİ

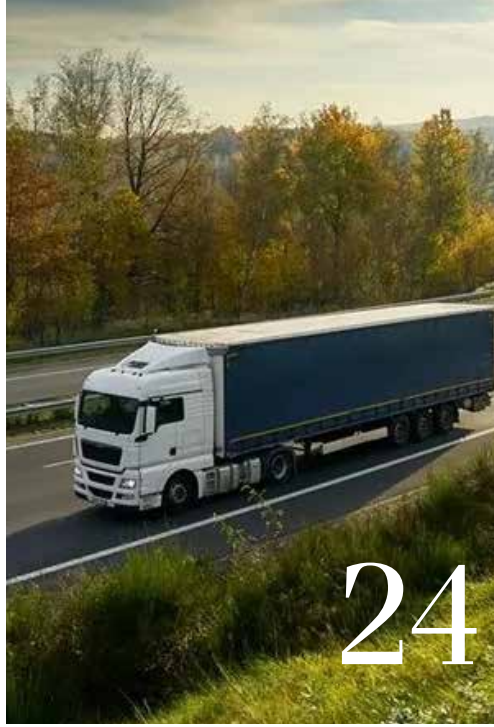
arkho
Tanıtım Hizmetleri

www.guvenlikyonetimi.com

içindekiler



20



24



34



4 BAŞKAN

6 EDITÖR

8 GÜNCEL

Sektör ile ilgili kısa haberler

18 KÖŞE / Hayata Bakış

SEKTÖRDEN

- 20 Modern Yaşam Alanlarında 360° Riskten Arınma Yaklaşımı

KAPAK ULAŞIM GÜVENLİĞİ

- 24 Karayolu Taşımacılığında Güvenlik Önlemleri
28 Ağır Yük Taşımacılığında Güvenlik Önlemleri
33 Yol Kullanıcılara Yönelik Eğitimler

FOKUS TÜNEL UYGULAMALARI

- 34 Tünellerin güvenliği
40 Avrasya Tüneli'nde bütüncül güvenlik önlemleri

ÖZEL DOSYA HEMŞİRE ÇAĞRI SİSTEMLERİ

- 42 2026 hemşire çağrı sistemleri pazarı
52 Sağlık Hizmetlerinde Yapay Zekâ Destekli Akıllı Sensör Teknolojisi

ELEKTRONİK GÜVENLİK

- 54 Fabrikalarda Yapay Zekanın Başarısı Veri Mimarisinden Geçiyor
58 BGüvenlik teknolojilerinde sürdürülebilirlik artık satın alma kriteri haline geliyor
50 Savunma ve Havacılıkta Üretimin Şartı Entegre ve İzlenebilir Dijital Altyapı

HAZİRAN 2026



54



66

GÜVENLİK HİZMETİ

- 58 Özel güvenlik hizmetlerinin meslek olarak kabul görebilmesi için özlük hakları iyileştirilmeli

YANGIN GÜVENLİĞİ

- 62 Yangın algılama ve ihbar sistemleri

BİLGİ GÜVENLİĞİ

- 66 Siber Saldırganların Kimlik Bilgilerine Dayalı Saldırı Teknikleri
- 68 Yapay zekâ doktorunuz değil, danışırken dikkat edin
- 70 Açığa Çıkan IP Adresleri Dijital Kimlikleri Tehdit Ediyor
- 72 Akıllı gözlükler güvenlik riski taşıyor

74 Editoryal takvim

75 Reklam indeksi

Özel Güvenlik Federasyonu adına imtiyaz sahibi
O. Oryal ÜNVER

Yürütme Kurulu
O. Oryal ÜNVER
İsmail UZELLİ
Murat Kösereisöğlü
Levent GÜLER
Alp SAUL

Genel Yayın Yönetmeni
Devrim BOZKURT
devrim@guvenlikyonetimi.com

Yazı İşleri
info@guvenlikyonetimi.com

Danışma Kurulu
Alp SAUL
Prof. Dr. Gazi UÇKUN
Deniz GÜRKAN
Engin ŞAHİN
Faruk DOĞAN
Hakan ÖZALP
İsmail UZELLİ
Murat Kösereisöğlü
O. Oryal ÜNVER
Yusuf Ziya ÖNCEL

Görsel Yönetmen
Derya BOZKURT
derya@guvenlikyonetimi.com

Reklam Müdürlü
Nazlı ÇATAK
info@guvenlikyonetimi.com

Yayın Türü
Yerel Süreli Yayın.
Ayda bir yayınlanır.

Yönetim Adresi
Arke Tanıtım Hizmetleri
Eyüpsultan - İstanbul
Tel: 0542 250 72 49
0533 413 78 08



Özel Güvenlik Sektörünün sesi Güvenlik Yönetimi Dergisi, sektörü bilgilendirme amacıyla hazırlanmıştır. Bu dergide yer alan her türlü haber, bilgi ve yorumlar; güvenilir olduğuna inanılan kaynaklar tarafından hazırlanmış araştırma raporları, değerlendirmeler, atıflar, çeviriler ve istatistikî verilerden derlenmiştir. Dergide yer alan tüm reklamların sorumluluğu firmalara, yazılardaki ve söyleşilerdeki görüşler sahibine aittir. Dergide yer alan yazılar izin alınmadan ve kaynak gösterilmeden hiçbir şekilde kullanılamaz.

Türkçeye gösterilecek özen, geleceğimize yapılan en değerli yatırımlardan biridir.

Değerli okurlarımız;

Günümüzde yazışmalarda ve günlük iletişimde yabancı kökenli, özellikle İngilizce sözcük ve terimlerin giderek daha yaygın kullanıldığını görüyoruz. Oysa dil, bir milletin kimliğinin, kültürünün ve bağımsızlığının en güçlü dayanaklarından biridir.

Geleceğe güvenle bakabilmemiz ve millî varlığımızı koruyabilmemiz için Türkçemize sahip çıkmak hepimizin ortak sorumluluğudur. Türkçenin doğru, özenli ve mümkün olduğunca yabancı sözcüklerden arındırılmış bir anlayışla kullanılması, kültürel varlığımızın ve toplumsal hafızamızın korunması açısından büyük önem taşımaktadır.

Türkçe yalnızca bir iletişim aracı değil; tarihimizin, düşünce dünyamızın ve millî kimliğimizin en güçlü taşıyıcısıdır. Dilimize sahip çıkmak, kültürümüze, geçmişimize ve geleceğimize sahip çıkmaktır.

Nazik değerlendirmeniz için teşekkür eder, çalışmalarınızda başarılar dilerim. Özellikle gençlere yönelik eserlerinizde Türkçenin doğru, güzel ve özenli kullanımına verdiğiniz önem son derece kıymetlidir. Bu duyarlılığınızın gelecek kuşaklara örnek olacağına yürekten inanıyorum.

Sağlıklı, güvenli ve mutlu yarınlar dileklerimizle...



O. Oryal ÜNVER
ÖGF (Özel Güvenlik Federasyonu)
Yönetim Kurulu Başkanı

“Yabancı sözcüklerin hızla yaygınlaştığı günümüzde Türkçeyi doğru ve özenli kullanmak, yalnızca bir dil meselesi değil; kültürümüzü, kimliğimizi ve geleceğimizi korumanın ortak sorumluluğudur.”

Akıllı binalar için kalıcı çözümler...

Yangın ve CO Alarm Sistemleri
IP CCTV Sistemleri
Kartlı Giriş Kontrol Sistemleri
Acil Anons Sistemleri
HVAC Mekanik Otomasyon Sistemleri
Enerji Otomasyon Sistemleri
KNX Aydınlatma Otomasyon Sistemleri

Sistemler Arası Entegrasyon

Smart **Struxure**



Powered by
StruxureWare™ Building Operation

matriks

BİNA KONTROL SİSTEMLERİ

www.matrikstr.com



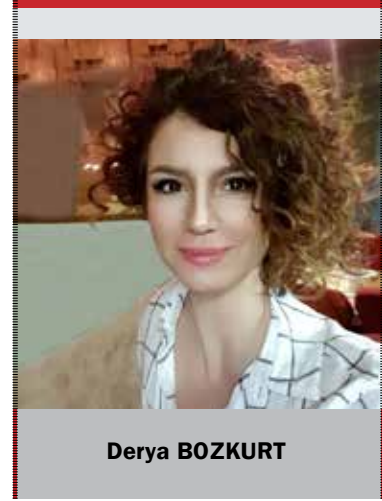
Haziran 2026 sayımızdan...

Haziran 2026 sayımızdan merhaba,
Kapak bölümümüzde **ULAŞIM GÜVENLİĞİ**'ni işledik.
"Karayolu taşımacılığında güvenliği sağlayan en kritik unsurlardan biri, sürücünün dikkatli ve bilinçli hareket etmesidir. Sürücüler, trafik kazalarının önlenmesinde ve taşınan yüklerin güvenli bir şekilde hedefe ulaşmasında kilit rol oynar. Bu nedenle, sürücülerin eğitilmiş olması, yasal kurallara uyması ve dinlenme düzenine dikkat etmesi gerekir."

Fokus bölümümüzün konusu ise **TÜNEL UYGULAMALARI** "Karayolları Genel Müdürlüğü 2005 yılında kurmuş olduğu bir komisyonla 2004/54/EC sayılı karara uygun olarak çalışmalar başlatmıştır. Özellikle tünellerde ağır yük taşımacılığı ve tehlikeli madde taşımacılığına yönelik risk analizi çalışmaları yapılmıştır." haberin devamını dergimizin sayfalarından keyifle okuyabilirsiniz.

Özel Dosya Konusu bölümümüzde ise **HEMŞİRE ÇAĞRI SİSTEMLERİ**. Modern hastanelerde güvenlik yalnızca bina girişlerini kontrol etmekten ibaret değildir. Hastanın yatağından yaptığı tek bir çağrı, yoğun bakımda saniyeler içinde verilen bir alarm ya da sağlık çalışanının maruz kaldığı şiddet sırasında bastığı panik butonu, doğrudan insan hayatını etkileyen kritik güvenlik süreçlerinin başlangıcıdır. Günümüzün IP tabanlı hemşire çağrı sistemleri; hasta güvenliği, personel güvenliği ve acil durum yönetimini tek bir platformda buluşturarak sağlık tesislerinin vazgeçilmez altyapılarından biri haline gelmiştir.

Keyifli okumalar...



Derya BOZKURT

“ İnsan, ölümünü bilen tek varlıktır. Ve tam da bu yüzden gerçekten yaşayabilir. Çünkü ölüm, hayatı sınırlı yapar. Bu yüzden ölümü unutmak otantik yaşamayı engeller. ”



Gördüğünüze inanın, göremediğinizi ona bırakın



Stadyum, şehir meydanı, deniz ve hava limanı gibi büyük ve kalabalık alanlarda yüksek çözünürlüğe sahip **Avigilon H5 Pro** ile üst düzey izleme ve kayıt yapılabilir. Sahip olduğu ileri seviye çözünürlük sayesinde her detayın incelenebilmesine olanak veriyor.

- 61 MP'ye kadar çözünürlük
- Video analiz yeteneği
- Gece görüşü

Detaylı bilgi için bizimle iletişime geçin:
www.y3k.com.tr



Securitas, Güvenlik Metodolojisi ile Fark Yaratıyor

Güvenlik hizmetlerinde fark yaratan en kritik unsurların başında, doğru kurgulanmış ve sürdürülebilirliği esas alan bir metodoloji geliyor. Securitas sahada yıllar edindiği deneyim ve bilgi birikimiyle geliştirdiği “Securitas Güvenlik Metodolojisi” ile sektörde önemli konulara rehberlik etmeye devam ediyor. Şirket, 2023 senesinde yayınladığı ve güvenlik hizmetlerinin planlanmasına, yönetimine ilişkin özel yaklaşımları paylaştığı kitabın bu sene uygulama kitabını yayınlamaya hazırlanıyor. Sektör profesyonellerinin kullanımına sunulacak olan kitapta Securitas Güvenlik Metodolojisinin nasıl uygulanması gerektiği tüm detaylarıyla yer alacak.

Securitas Güvenlik Metodolojisi; risk analizi, süreç tasarımı, insan kaynağı planlaması ve teknoloji entegrasyonunu tek bir çatı altında ele alan bütüncül bir bakış açısı sunuyor. Bu

yapı sayesinde kurumlara özel, optimize edilmiş ve ölçülebilir güvenlik çözümleri geliştiriliyor. Metodolojinin en önemli özelliklerinden biri ise güvenliği statik bir hizmet olarak değil, değişen koşullara uyum sağlayabilen dinamik bir sistem olarak ele alması. Bu yaklaşım, özellikle farklı operasyonel fazlara sahip projelerde güvenlik süreçlerinin daha etkin yönetilmesine katkı sağlıyor.

Güvenlik hizmetlerini kurgularken bu metodolojiyi merkeze aldıklarına dikkat çeken Securitas Türkiye Ülke Başkanı Murat Kösereisioğlu, “Securitas Güvenlik Metodolojisi, bizi rakiplerimizden ayıran en önemli unsurlardan biri. Hizmet optimizasyonu için yapılması gerekenleri sistematik şekilde tanımlarken sürdürülebilirliği, dijital dünyayı ve teknoloji entegrasyonunu sürecin merkezine yerleştiriyoruz” dedi.

Securitas Türkiye’nin en önemli güçlerinden birinin sektörel uzmanlaşma olduğunu belirten Kösereisioğlu, “Bugün Türkiye genelinde 22 bini aşkın çalışanımızla 29 farklı sektörde hizmet veriyoruz. Bu deneyim, metodolojimize sektöre özgü riskleri ve çözüm yaklaşımlarını dahil etmemizi sağlıyor” diye konuştu.

Küresel Deneyimle Şekillenmiş Güvenlik Yaklaşımı

Securitas’ın güvenlik metodolojisinin temelinde, dünyanın farklı coğrafyalarında ve farklı sektörlerde elde ettiği küresel deneyim yer alıyor. Uluslararası



bilgi birikimini yerel uzmanlıkla birleştiren şirket, dünyanın önde gelen kuruluşlarına, kritik altyapı projelerine ve yüksek güvenlik gerektiren operasyonlara özel çözümler geliştiriyor. Farklı ülkelerde edinilen operasyonel tecrübeleri Türkiye’ye taşıyan Securitas; üretim tesislerinden veri merkezlerine, enerji altyapılarından lojistik operasyonlarına, havalimanlarından büyük ölçekli etkinliklere kadar birçok alanda kuruma özel güvenlik modelleri tasarlıyor. Bu çözümler; risklerin doğru analiz edilmesi, kaynakların etkin kullanılması ve teknolojinin operasyonlara entegre edilmesi prensiplerine dayanıyor. Konuyla ilgili değerlendirmede bulunan Murat Kösereisioğlu, “Securitas olarak yalnızca Türkiye’deki deneyimimizden değil, dünyanın farklı noktalarında edinilen bilgi birikiminden de besleniyoruz. Bu sayede müşterilerimize uluslararası standartlarda, sektörün ve operasyonun ihtiyaçlarına özel tasarlanmış güvenlik çözümleri sunabiliyoruz” dedi.



Para ve değerli eşyalarınızın güvenliğine odaklanırken
maliyetinizi azaltıyor,
risklerinizi devralıyor,
zaman kaybınızı önüyoruz.

0212 603 03 70



www.loomis.com.tr



Managing **cash** in society.

Geleceğin Sanayisi Sürdürülebilir Olacak

İklim krizi ve küresel çevre politikaları üretim dünyasında yeni bir yol haritası oluşturuyor. Çevresel etkiyi azaltan, kaynak verimliliğini artıran ve sürdürülebilirliği merkeze alan uygulamalar sanayinin geleceğini şekillendirirken, Türkiye'nin ilk Kimya İhtisas Organize Sanayi Bölgesi GEBKİM OSB ise Yeşil OSB vizyonu ile sanayide sürdürülebilir dönüşümün dikkat çeken örnekleri arasında yer alıyor.

Türk Standartları Enstitüsü (TSE) tarafından yürütülen Yeşil OSB Sertifikasyon Programı kapsamında "Yeşil OSB" unvanını alan GEBKİM OSB; enerji ve su verimliliği, atık yönetimi, yenilenebilir enerji uygulamaları ve çevre dostu altyapı yatırımlarıyla çevre odaklı üretim anlayışını sürdürüyor.

Sürdürülebilirlik Artık Ekonomik Güç Unsuru

Küresel pazarlarda çevre standartlarının hızla yükselmesi, sanayide sürdürülebilirlik yatırımlarını da zorunlu hale getiriyor. Düşük karbon ekonomisine geçiş sürecinde enerji verimliliği, su tasarrufu, atık azaltımı ve çevresel yönetim sistemleri yalnızca çevreyi koruyan uygulamalar değil; aynı zamanda şirketlerin uluslararası rekabet gücünü artıran stratejik başlıklar olarak öne çıkıyor. Sanayi ve Teknoloji Bakanlığı ile Dünya Bankası iş birliğiyle oluşturulan Yeşil OSB Sertifikasyon Programı da bu dönüşümün en önemli adımları arasında gösteriliyor. Program kapsamında enerji verimliliği, sıfır atık uygulamaları, çevresel yönetim sistemleri ve



sürdürülebilir altyapı yatırımları gibi birçok kriter değerlendiriliyor.

Üretimden Toplumsal Faydaya Uzanan Model

Çevresel sürdürülebilirliği yalnızca üretim süreçleriyle sınırlı görmeyen GEBKİM OSB; sosyal sorumluluk projeleri, kaynak verimliliği uygulamaları ve çevre odaklı yatırımlarla sürdürülebilirlik yaklaşımını daha geniş bir çerçevede ele alıyor.



Avrupa'nın En Kapsamlı Risk Önleme ve Güvenlik Fuarı

3 - 5 Kasım 2026 Paris Porte de Versailles, Fransa

Expoprotection 2026

İş güvenliği, yangın koruma, siber güvenlik ve risk yönetimi alanlarında Avrupa'nın en prestijli etkinliklerinden biri olan **Expoprotection 2026**, sektör liderlerini, üreticileri, çözüm sağlayıcılarını ve kamu temsilcilerini Paris'te bir araya getiriyor.

Bu etkinlik; çalışan güvenliğinden çevresel risklere, dijital tehditlerden yangın önlemeye kadar çok geniş bir yelpazede çözümler sunuyor.





PRONET+

TÜM GÜVENLİK SİSTEMİNİ
TEK UYGULAMADAN YÖNETTİĞİN
EVİNE GÜVEN



444 1 911
pronet.com.tr

Uç nokta korumasında fark yaratan başarı



Siber güvenlik alanında dünya lideri olan ESET, ESET PROTECT ürünüyle 2026 Gartner® Magic Quadrant™ for Endpoint Protection1 raporunda üst üste üçüncü kez

Challenger olarak gösterildi. ESET, raporda 16 yıl üst üste yer aldı ve son 8 baskıda 7 kez “Challenger” olarak adlandırıldı.

ESET, rekabetçi fiyatlandırma ve kanıtlanmış uzun vadeli performansın da desteğiyle güçlü uygulama ve kapsamlı vizyonun konumunu belirlediğine inanıyor.

ESET İşletme Direktörü Pavol Balaj, “2026 Uç Nokta Koruması için Magic Quadrant’ta tek ‘Challenger’ olarak gösterilmek, bizim açımızdan stratejimizin ve dünya çapındaki müşterilerimize sunduğumuz değer in güçlü bir teyidi niteliğinde. Bunu, tutarlı inovasyonumuzun, güçlü performansımızın ve siber güvenliği hem etkili hem de yö-

netimi kolay hâle getirmeye olan bağlılığımızın bir takdiri olarak görüyoruz. Kuruluşların gelişen siber tehditlerin bir adım önünde olmalarına yardımcı olmak için platform yeteneklerimizi geliştirmeye yatırım yapmaya devam edeceğiz. Gartner, “Challenger”lar, uç nokta koruması satın alanların ihtiyaçlarını etkili bir şekilde karşılayan olgun uç nokta koruma ürünleri sunar. Ayrıca pazarda güçlü bir görünürlükleri vardır, bu da Niche Players’a kıyasla daha iyi bir Yürütme Yeteneği ile sonuçlanır. Challenger’lar, özellikle onlarla sağlam stratejik ilişkiler kurmuş müşteriler için pratik seçimlerdir” açıklamasını yaptı.

TCK By Kırac’tan Avrupa Savunma Sanayisine Stratejik Hamle

Türkiye’nin sanayi ve mühendislik alanındaki yükselen markalarından Tck By Kırac AŞ, gerçekleştirdiği stratejik yatırımlar ve uluslararası iş birlikleriyle savunma sanayisindeki büyümesini küresel ölçekte hızlandırıyor.

İstanbul’da düzenlenen SAHA EXPO 2026 kapsamında Norveç merkezli Nordic Deployment AS ile stratejik iş birliği anlaşması imzalayan şirket, şimdi de Avrupa’nın en önemli savunma sanayi organizasyonlarından biri olan HEMUS 2026 Uluslararası Savunma Ekipmanları ve Hizmetleri Fuarı’nda yer alarak Avrupa ve NATO pazarlarına yönelik büyüme hedeflerini uluslararası platformda ortaya koyuyor. Bulgaristan’ın Plovdiv kentinde düzenlenen ve NATO ülkeleri ile Avrupa savunma sanayi ekosisteminin önde gelen

temsilcilerini bir araya getiren HEMUS 2026 Fuarı’nda Tck By Kırac AŞ; savunma sanayisine yönelik geliştirdiği yüksek mukavemetli çelik çözümlerini, stratejik üretim altyapısını ve ileri mühendislik kabiliyetlerini uluslararası sektör temsilcileriyle buluşturuyor. Gerçekleştirdiği yatırımlar ve uluslararası iş birlikleri sayesinde Avrupa Birliği ülkeleri, Balkanlar ve NATO coğrafyasındaki projelerde daha güçlü şekilde yer almayı hedefleyen Tck By Kırac AŞ, HEMUS 2026 kapsamında gerçekleştireceği görüşmelerle yeni ihracat fırsatları ve stratejik ortaklıklar geliştirmeyi amaçlıyor.

Fuar kapsamında yapılacak temaslarda şirketin uluslararası büyüme stratejisine önemli katkılar sağlaması ve Avrupa savunma sanayisi ekosistemindeki konumu-



nu güçlendirmesi bekleniyor. Serkan Malçok açıklamasını şu sözlerle tamamladı: “Biz yalnızca bugünü üretmiyoruz. Geleceğin stratejik altyapılarını, güvenlik sistemlerini ve mühendislik çözümlerini inşa ediyoruz. Hedefimiz Tck By Kırac’ı bölgesel bir üreticiden çıkararak dünya çapında tanınan bir savunma, enerji ve stratejik altyapı markasına dönüştürmektir. Türkiye’nin üretim gücünü küresel sahnede daha güçlü temsil etmeye devam edeceğiz.”

Huzurlu bir yaşam arıyorsan...



Daha fazla
bilgi için
QR kodu okutun.

Biz buradayız.



Gençlere Güvenen Şirketler Daha Hızlı Büyüyor

Küresel ekonomideki dalgalanmalar ve artan maliyet baskısı, şirketleri daha kontrollü ve esnek iş modellerine yönlendiriyor. Türkiye’de e-ticaret büyümeye devam ederken, sektörde rekabetin çerçevesi de yeniden şekilleniyor. Bu yeni tabloda öne çıkanlar; kaliteli üretimi sürdüren, fiyatı ulaşılabilir seviyede tutabilen ve tüketiciyle güven ilişkisi kurabilen yapılar oluyor.

Pandemi sonrası hızlanan dijitalleşme süreciyle birlikte şirketler, veri odaklı sistemler üzerinden tüketici davranışlarını daha yakından analiz etmeye başladı. Bu dönüşüm yalnızca üretim ve satış süreçlerini değil, ürün sonrası kullanıcı deneyimini de iş modelinin önemli bir parçası haline getirdi. Lojistik süreçlerinden müşteri ilişkilerine kadar uzanan

yapı, şirketlerin güven algısını doğrudan etkileyen temel unsurlar arasında yer alıyor. Bu yeni yaklaşımın dikkat çeken örneklerinden biri olan Adoba Global, üretim ve e-ticareti aynı yapı altında yürüten şirketler arasında yer alıyor. Yaklaşık 1000 kişilik çalışan kadrosuyla faaliyetlerini sürdüren şirket; genç çalışanlara alan açan organizasyon yapısı, veri odaklı karar süreçleri ve hızlı aksiyon alma kabiliyetiyle değişen rekabet koşullarına uyum sağlayan yapılar arasında öne çıkıyor. Yeni nesil kullanıcı davranışlarının hızla değiştiği bir dönemde, genç ekiplerle çalışan şirketler pazarındaki beklentileri daha hızlı analiz edebiliyor. Değişen ihtiyaçlara kısa sürede yanıt verebilmek, esnek



hareket edebilmek ve karar alma süreçlerini hızlandırmak şirketlere önemli avantajlar sağlıyor. Sektörde bu yaklaşımı benimseyen şirketlerden biri olan Adoba Global, genç çalışanlarını karar süreçlerine dahil eden yapısıyla dikkat çekiyor. Genç ekiplerin dinamizmi ve sahadaki değişime hızlı adaptasyonu, şirketlerin pazara daha kısa sürede yanıt verebilmesini sağlıyor.

Siber dayanıklılık için küresel iş birliği



Siber uzayda ve dijital alanda caydırıcılık ve savunma, yalnızca güvenilir donanım ve yazılım meselesi değil, aynı zamanda NATO Siber ve Dijital Dönüşümünden Sorumlu Genel Sekreter Yardımcısı Jean Ellermann-Kingombe’nin de ifade ettiği gibi, ortak normlar ve ilkelerle de ilgili. Bu durum, toplumların işleyişi için hayati

önem taşıyan kritik altyapının saldırı altında olduğu ve kötü niyetli aktörlerin teknolojik gelişmelerden yararlanarak taktiklerini hızla geliştirdiği bir dönemde özellikle geçerli. Bu stratejik, ticari olmayan ortaklıklar Estonya’nın Tallin kentinde düzenlenen Uluslararası Siber Çatışma Konferansı’nda (CyCon) resmen duyuruldu ve NATO ile sanayi arasındaki siber iş birliğine yeni bir ivme kazandırdı. Bu ortaklıklar, diyalogu, bilgi paylaşımını, en iyi uygulamaların değiş tokuşunu ve ortak ilgi alanlarına yönelik koordineli faaliyetleri kolaylaştırmaya yardımcı olacak. Kurumsal Çözümler Direktörü Martin Talian, “Ne yazık ki toplumumuzu zayıflatmaya ve

değerlerimizi sorgulamaya çalışan siber tehditlerin giderek arttığı bir dönemde yaşıyoruz; bu nedenle, bu tehditlere karşı dayanıklılığı iş birliği içinde artırmayı amaçlayan bu önemli girişime katılmaktan büyük memnuniyet duyuyoruz” açıklamasını yaptı. ESET, siber uzayı daha güvenli hâle getirme rolü kapsamında çalışmalarını yürütmektedir. Üstlendiği bu misyon kapsamında tehdit ortamına ilişkin benzersiz küresel görüşünden, Ukrayna gibi çatışma bölgeleri de dâhil olmak üzere kritik altyapıyı koruyan siber güvenlik uzmanlarına sağladığı destekten ve en ileri teknolojilerle donatılmış, sürekli genişleyen araştırma ekiplerinden yararlanmaktadır.

Exit



Musical Fountain



boutique



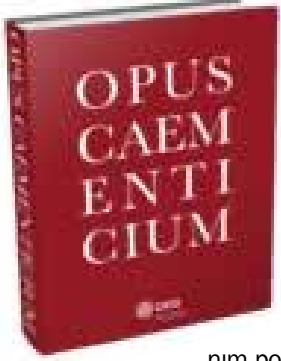
**GÜVENLİK,
DETAYLARI GÖRME SANATIDIR!**



Detaylar için
QR kodu okutunuz.



Çimentonun Mimarlık İçindeki Yolculuğu Kitaplaştı: Opus Caementicium



ÇEİS tarafından yayımlanan "Opus Caementicium" kitabı, çimento ve betonun mimarlık tarihindeki yerini ve çağdaş mimarlıktaki kulla-

nım potansiyellerini farklı dönemlerden örneklerle ele alıyor. Çimento Endüstrisi İşverenleri Sendikası (ÇEİS) ile Binat Mimarlık Medya Grubu iş birliğiyle, Arredamento Mimarlık dergisinde beş yıl boyunca yayımlanan yazı dizisinin kitaplaştırılmasıyla hazırlanan "Opus Caementicium" çimento ve betonun teknik bir yapı malzemesi olmanın ötesine geçerek mimarlık düşüncesi ve yapı kültürü içindeki çok katmanlı rolünü ele alıyor. ÇEİS'in kurumsal iletişim çalış-

maları kapsamında ortaya çıkan bu yayının, malzemenin mimarlık pratiği içindeki yerini yeniden düşünmeye davet eden bir kaynak olması hedefleniyor.

ÇEİS tarafından desteklenen bu çalışma, sektör ile mimarlık dünyası arasında karşılıklı öğrenmeye dayalı bir etkileşim alanı oluşturmayı hedefliyor. Çimento ve betonun nitelikli kullanımının teşvik edilmesi, mimarlık pratiğinde malzeme bilincinin güçlendirilmesi ve yapı kültürüne katkı sunulması, kitabın temel yaklaşımını oluşturuyor. Aynı zamanda çalışma, malzemenin tasarım sürecinin erken aşamalarından itibaren bilinçli ve yaratıcı biçimde ele alınmasının, mimari kaliteyi yükseltmekle birlikte yapıyı çevrenin daha sürdürülebilir, uzun ömürlü ve kültürel açıdan değerli hale gelmesine katkı sunduğunu ortaya koyuyor.

Saldırlara karşı korunmayı güçlendirme adımları

Mevcut güvenlik kontrollerinizi Kaspersky Managed Detection and Response (MDR) gibi insan odaklı tespit yetkinlikleriyle güçlendirin ve Kaspersky Incident Response hizmetiyle güvenlik olaylarına ilişkin kapsamlı analizler elde edin. Bu hizmetler, tehditlerin tespitinden sürekli koruma ve iyileştirmeye kadar tüm olay yönetimi sürecini kapsayan 7/24 izleme sunar. Kurum içi süreç ve teknolojilerinizi, sürekli evrilen tehdit ortamına uyumlu hale getirmek için Kaspersky SOC Consulting hizmetinden yararlanın. Bu hizmet, sıfırdan bir SOC kurulmasına, mevcut SOC yapısının olgunluk seviyesinin değerlendirilmesine veya tespit ve müdahale süreçleri gibi belirli yetkinliklerin geliştirilmesine destek olur.

Tüm varlıklarınızı kapsayan bütüncül koruma sağlamak için Kaspersky Next XDR Expert gibi merkezi ve otomatik çözümler kullanın. Farklı kaynaklardan gelen verileri tek bir noktada toplayıp ilişkilendirerek ve makine öğrenimi teknolojilerinden yararlanarak etkili tehdit tespiti ve hızlı otomatik müdahale imkânı sunar.

Dijital Bağımlılık Duygu Durumunu Etkiliyor

Ekran bağımlılığı; bireyin cihaz kullanımını kontrol edememesi ve bu durumun günlük yaşam işlevlerini olumsuz etkilemesiyle ortaya çıkan bir tablo. Sadece ekran süresi değil, kullanımın sınırlandırılmaması ve cihazdan uzak kalındığında hissedilen huzursuzluk, gerginlik ve boşluk duygusu da bu bağımlılığın temel göstergeleri arasında gösteriliyor. Bu durum; dikkat eksikliği, uyku sorunları, sosyal izolasyon, kaygı ve depresyon gibi sorunlarla yakından ilişkili. Çocuklarda stres, yalnızlık ve duygusal yorgunlukla başlayan ekran kullanımı, zamanla duyguları düzenlemenin temel aracı haline gelebiliyor. Özellikle sosyal

medyada sürekli onay arayışı ve kıyaslama, çocukların özgüvenini düşürürken kaygılarını da artırıyor.

Dijital bağımlılıkların temelinde yatan şey, beynimizin ödül sistemi. Çünkü insan beyni, haz veren davranışları tekrar etmeye eğilimli. Dijital oyunlar ve sanal platformlar da kullanıcıya belirsiz aralıklarla ödül sunacak şekilde tasarlandığı için bu belirsizlik, dopamin salgılamasını tetikleyerek kısa süreli bir haz sağlıyor ve davranışın tekrarını güçlendiriyor. Zamanla bu döngü, alışkanlığa ve kontrolsüz kullanıma dönüşebiliyor. İstanbul Okan Üniversitesi Hastanesi'nden Uzm. Klinik Psikolog M. Yasin Çakıroğlu, dijital bağımlılıkla baş-

etme sürecinin, atılacak 3 adımla doğru yönetilmesi gerektiğini vurguluyor:

Farkındalık Geliştirin: Dijital kullanımın hangi duygular ve durumlar tarafından tetiklendiğini anlamak, değişimin ilk adımıdır. **Günlük Yaşamı Yeniden**

Düzenleyin: Düzenli uyku, sağlıklı beslenme, fiziksel aktivite ve sosyal ilişkilerin güçlendirilmesi bağımlılıkla mücadelede önemli rol onar. Dijital olmayan aktiviteler, alternatif mutluluk kaynakları oluşturur. **Profesyonel Destek Alın:** Bilişsel davranışçı terapi (BDT) ve motivasyon artırıcı terapiler, dijital ve sanal kumar bağımlılığı tedavisinde etkili yöntemler arasında yer alır. Gerekliğinde ilaç tedavisi de sürece dâhil edilebilir.

TEPE
GÜVENLİK

TEPE'DE
YENİ DÖNEM



TEPE
KURUMSAL

444 15 98
tepekurumsal.com.tr

“Etkili liderlik”

Kişisel bütünlük, kişisel sorumluluk ve yaşam amacının ufkundaki aydınlık geleceğimizi oluşturur. Kişisel bütünlük kişisel sorumlulukla beslenir. Böylece siz kararlı ve eyleme dönük bir kişi olmak istediğinizde, kişisel bütünlüğünüz yaşam amacınızı canlı tutar.

Amacınıza dayalı sorumlu bir yaşam sürdürdükçe bilgeliliğiniz de artar. Kişisel bütünlüğü kendinizde ve birlikte çalıştığınız kişilerde arayın. Kişisel ve mesleki ilişkilerinizin güven temeline dayanmasını sağlayan unsurlar, karşılıklı saygı ve kişisel bütünlüktür. Kişisel bütünlüğünüz, anne-baba, yönetici, satış elemanı, lider, iş sahibi, işçi, eş veya öğretmen olarak “ya da başka bir işte” ne kadar etkili olacağınızı belirler. Kişisel bütünlüğünüz, elde edeceğiniz gerçek başarının ölçüsüdür.

Her toplumda, kargaşanın başlıca nedenlerinden birisi, politik ve ekonomik alandaki liderlerin kişisel bütünlüklerinin olmamasıdır. Biz kişisel bütünlüğe sahip liderler istiyoruz, önemli pozisyonlarda kişisel sorumluluğa sahip insanların bulunması gerekir. Hükümetlerde, işletmelerde, ailelerde ve diğer kurumlarda bu tür liderlere gereksinim vardır. Liderliğin iyi olmasını engelleyen unsurlar; etkisiz liderler de, etkili liderlerin önüne çıkan engellerle karşılaşır. Etkili liderler, azim ve yaratıcılıkla engelleri nasıl aşacaklarını öğrenirler. Etkisiz liderlerin etkili olabilmeleri için, eylemlerinin sorumluluğunu üstlenmeyi öğrenmeleri gerekir. Bu kişiler genelde, toplumun içi boş olan başarı tanımına denk düşmeme korkusu yaşarlar. Bu korku, kişisel bütünlüklerini tehlikeye atar. Bir hedefe ulaşmak için başkalarını ezebilir ya da ilişkilerinde yalana dolana sapabilirler. Korkuları, davranışlarının sonuçlarının sorumluluğunu inkâr etmelerine yol açabilir. Yaptıklarının yanlış olduğunun bilinciyle, cezalandırılmaktan hatta işlerini kaybetmekten kaçınıyor olabilirler. Bu da, kişiliklerinin iç yüzünün anlaşılması korkusuyla hareket etmelerine yol açabilir. Ayrıca sorumluluktan kaçarak ve korkularıyla hareket ederlerse alacakları sonuçlar da hiç iç açıcı olmaz ve bu sonuçlar onları tatmin etmez.

Anne ve babaları düşündüren şey, tutarlı ve etkili bir disiplin kurmaktan çok, çocuklarının kendilerini beğenmesi ve kendilerine itaat etmesidir. Çocuklar, disiplin olmadan nasıl kişisel sorumluluğa dayanan alışkanlıklar kazanacaklar ve ileride kişisel bütünlüğe sahip yetişkinler olacaklardır? Bir anne veya baba olarak, sözleriniz ve davranışlarınızda tutarlı değilseniz, çocuğunuzun saygısını nasıl kazanırsınız?

Aynı durum yönetici ve liderler için de geçerlidir. İnsanların kendilerini beğenmesine odaklananlar, genelde zayıf, etkisiz ve tutarsız birer insan olurlar. Bir yönetici veya lider olarak, sözleriniz ve davranışlarınızda tutarlı değilseniz, çalışanlarınızın ya da liderlik yaptığınız kişilerin saygısını nasıl kazanırsınız? “Kişisel bütünlük, etkili liderliğin anahtarıdır”. Güven kişisel bütünlükle yaşayan kişiye, başkaları tarafından verilen bir armağandır.



Oğuz GÜLAY

“Her toplumda, kargaşanın başlıca nedenlerinden birisi, politik ve ekonomik alandaki liderlerin kişisel bütünlüklerinin olmamasıdır.”

Başarabilmemiz dileği ile...

Değişimi birlikte yakalayalım...



Creative
Çözümler

Logo
Amblem
Tasarım

Kurumsal
Kimlik
Tasarımı

Katalog,
Broşür
Tasarımı

Ambalaj
Tasarımı

Basın İlanı
Tasarımı

Broşür
ve Insert

Baskı
Çözümleri

Güvenlik Yönetimi
ÖZEL GÜVENLİK SEKTÖRÜNDEN SESİ

Gündem
Perpa Sanayi ve Ticaret A.Ş. Adına
İstanbul Şişli Şişli Şişli

ARKHE TANITIM HİZMETLERİ
Perpa Ticaret Merkezi B Blok
Kat:6 No:672
Okmeydanı / Şişli / İstanbul
Tel : (212) 210 54 45
www.guvenlikyonetimi.com

arkhe
tanıtım hizmetleri

Modern Yaşam Alanlarında 360° Riskten Arınma Yaklaşımı

Güvenlik, yalnızca olay olduktan sonra kayıt izlenen bir sistem değil; riski önceden okuyan, doğru veriyi yöneten ve yaşam alanının değerini koruyan bütünlüklü bir yönetim disiplini.

İLGİ GÜVENLİK

Güvenlik teknolojileri son yıllarda yalnızca daha görünür hale gelmedi; aynı zamanda tesis yönetimlerinin karar alma biçimini de değiştirdi. Site, rezidans, kampüs, iş merkezi ve karma yaşam alanlarında güvenlik artık kapıda başlayan tek yönlü bir kontrol süreci olarak görülüyor. İnsan sirkülasyonu, araç girişleri, ziyaretçi yönetimi, teslimat akışı, otopark güvenliği, ortak alanların izlenmesi, teknik hacimlerin korunması ve çevre hattının kontrolü aynı güvenlik mimarisi içinde değerlendiriliyor. Bu dönüşümün temelinde, risklerin olay yaşandıktan sonra değil, henüz oluşmadan önce fark edilmesi ihtiyacı yer alıyor. Çünkü modern yaşam alanlarında güvenlik açığı yalnızca bir ihlal ya da olay anlamına gelmez; aynı zamanda kullanıcı deneyimini, tesis algısını, operasyonel verimliliği ve mülk değerini doğrudan etkileyen bir yönetim başlığıdır.



Güvenlik artık tek bir noktadan başlamıyor

Bugünün güvenlik anlayışında risk, çoğu zaman tek bir kapıdan, tek bir kameradan ya da tek bir alarm noktasından ibaret değildir. Risk; alanın kullanım yoğunluğu, kör noktalar, yetkisiz geçiş ihtimalleri, araç ve yaya trafiği, acil durum senaryoları ve verinin doğru saklanıp saklanmaması gibi birçok değişkenin birlikte değerlendirilmesiyle ortaya çıkar. Bu nedenle etkili güvenlik planı, yalnızca ekipman listesiyle

hazırlanamaz. Önce alanın günlük işleyişi okunmalı, sonra sahadaki insan kaynağı ile teknolojik altyapı aynı planın tamamlayıcı parçaları olarak kurgulanmalıdır. İLGİ Güvenlik'in 360° Riskten Arınma Yaklaşımı, tam da bu bütüncül ihtiyaca cevap veren bir model sunar.

360° bakış neyi değiştirir?

360° yaklaşım, güvenliği yalnızca izleme ve müdahale faaliyeti olarak ele almaz. Alanın yapısını,



kullanıcı alışkanlıklarını, giriş-çıkış yoğunluğunu, kritik noktalarını ve olası zafiyetlerini birlikte değerlendirir. Böylece güvenlik sistemi, tek tek çalışan araçlardan oluşan dağınık bir yapı olmaktan çıkar; ölçülebilir, denetlenebilir ve geliştirilebilir bir yönetim modeline dönüşür.

Proaktif CCTV ve izleme sistemleri, giriş-çıkış ve geçiş kontrol çözümleriyle birlikte çalıştığında sahadaki güvenlik ekibine yalnızca görüntü değil, anlamlı bir operasyon bilgisi de sağlar. Kritik nokta alarm sistemleri, çevre güvenliği ve ihlal tespitiyle desteklendiğinde ise riskli durumların daha erken fark edilmesi mümkün hale gelir.

Proaktif güvenlik: İzlemek-ten önce anlamak

Kamera sistemleri uzun süre boyunca geçmişe dönük inceleme aracı olarak konumlandırıldı. Bir olay yaşanır, ardından kayıtlar incelenir ve sürecin nasıl geliştiği anlaşılmaya çalışılırdı. Bugün ise CCTV sistemleri, güvenlik operasyonlarının aktif bir bileşeni haline geldi. Yüksek çözünürlüklü görüntüleme, daha gelişmiş kayıt altyapıları, uzaktan izleme imkânları ve merkezi yönetim çözümleri sa-

yesinde kameralar yalnızca kayıt alan cihazlar olmaktan çıktı. Proaktif CCTV yaklaşımında kamera, sahadaki risklerin daha erken fark edilmesini sağlayan stratejik bir gözlem noktasıdır. Yoğunluk artışı, şüpheli davranış, yetkisiz alana yaklaşma, çevre hattında olağan dışı hareket, terk edilmiş nesne ya da kritik noktada beklenmeyen durumlar güvenlik ekibinin dikkatine daha hızlı taşınabilir.

Geçiş kontrolü: Güvenli akışın görünmeyen omurgası

Modern tesislerde güvenliğin en kritik başlıklarından biri giriş-çıkış ve geçiş kontrolüdür. Çünkü bir alanın güvenli olup olmadığını belirleyen unsurlardan biri, kimin, ne zaman, hangi noktadan ve hangi yetkiyle giriş yaptığının takip edilebilmesidir. Geçiş kontrol çözümleri; personel, ziyaretçi, tedarikçi, servis sağlayıcı ve araç akışını düzenli bir yapıya bağlar. Bu sayede güvenlik yalnızca fiziksel kontrolle sınırlı kalmaz; kayıt altına alınabilir, raporlanabilir ve gerektiğinde geriye dönük olarak incelenebilir bir süreç haline gelir.

“Modern yaşam alanlarında güvenlik açığı yalnızca bir ihlal ya da olay anlamına gelmez; aynı zamanda kullanıcı deneyimini, tesis algısını, operasyonel verimliliği ve mülk değerini doğrudan etkileyen bir yönetim başlığıdır.

Alarm ve ihlal tespiti: Müdahaleden önce uyarı

Kritik nokta alarm sistemleri, güvenlik zincirinin erken uyarı mekanizmasıdır. Tek başına kamera kaydı bir ihlali gösterebilir; ancak alarm sistemi, güvenlik ekibini doğru anda harekete geçiren tetikleyici rolü üstlenir. Kapı zorlaması, yetkisiz giriş denemesi, çevre hattı ihlali, teknik alanda beklenmeyen hareket veya kritik ekipman bölgesindeki riskli durumlar alarm senaryoları içinde değerlendirilebilir.

Çevre güvenliği ve ihlal tespiti

Tesis güvenliğinde çevre hattı, çoğu zaman ilk savunma noktasıdır. Duvar, çit, bahçe sınırı, otopark girişi, servis yolu ve açık alanlar yalnızca fiziksel sınırlar değildir; aynı zamanda riskin ilk görülebileceği alanlardır. Entegre çevre güvenliği, bu noktaları kamera, algılama, aydınlatma, alarm ve saha devriyesiyle birlikte ele alır.



Veri kaydı ve arşivleme neden kritik?

Güvenlik yönetiminde veri kaydı yalnızca geçmişe dönük inceleme için tutulmaz. Doğru veri; denetim, raporlama, sorumluluk takibi, süreç iyileştirme ve karar alma mekanizmalarının temelini oluşturur. Hangi noktada yoğunluk olduğu, hangi saatlerde risk seviyesinin arttığı, hangi alanlarda ek önlem gerektiği ve hangi olayların tekrarlandığı ancak düzenli kayıt ve arşivleme ile görülebilir.

Yasal mevzuata uyumlu veri kaydı, modern güvenlik hizmetinin en hassas başlıklarından biridir. Görüntülerin, geçiş kayıtlarının ve olay raporlarının doğru sürelerde, doğru erişim yetkileriyle ve güvenli biçimde saklanması gerekir. Bu düzen yalnızca hukuki sorumlulukları karşılamak için değil; aynı zamanda tesis yönetiminin güvenlik süreçlerini şeffaf, izlenebilir ve denetlenebilir hale getirmesi için de gereklidir.

Sistem tasarımı ve projelendirme

Her yaşam alanının güvenlik ihtiyacı farklıdır. Aynı metrekareye sahip iki tesis bile kullanıcı profili, giriş yoğunluğu, çevre

yapısı, ortak alan kullanımı ve teknik altyapı bakımından birbirinden ayrılabilir. Bu nedenle standart paket çözümler çoğu zaman kalıcı güvenlik performansı üretmekte yetersiz kalır.

İnsan kaynağı ile teknolojinin aynı dili konuşması

Güçlü güvenlik yalnızca cihazlarla kurulmaz. Teknoloji, sahadaki ekibin doğru karar vermesini kolaylaştırdığı ölçüde değerlidir. Güvenlik görevlisinin hangi durumda nasıl aksiyon alacağını bilmesi, sistemden gelen uyarıyı doğru yorumlaması, kayıt ve raporlama düzenine uyması ve tesis yönetimiyle aynı operasyon dilini kullanması gerekir. Bu nedenle 360° Riskten Arınma Yaklaşımı, insan kaynağını ve teknolojiyi birbirinden bağımsız iki unsur olarak değil, aynı güvenlik ekosisteminin tamamlayıcı parçaları olarak ele alır. Eğitimli ekip, doğru sistem, düzenli kayıt, proaktif izleme ve ölçülebilir süreçler bir araya geldiğinde güvenlik sürdürülebilir hale gelir.

Güvenlik bir maliyet değil, yönetim değeridir

Modern yaşam alanlarında

güvenlik yatırımı, yalnızca olası kayıpları önlemeye yönelik bir maliyet kalemi olarak düşünülmemelidir. Güvenlik; yaşam kalitesini artıran, tesis değerini koruyan, yönetim süreçlerini güçlendiren ve kullanıcı memnuniyetini destekleyen stratejik bir hizmet alanıdır.

İLGİ Güvenlik ile sürdürülebilir güvenlik yaklaşımı

İLGİ Güvenlik, modern yaşam alanları için proaktif, ölçülebilir ve mevzuata uyumlu güvenlik modelleri geliştirir. Riskleri görünür kılmak, doğru sistemi kurmak ve güvenliği sürdürülebilir bir yönetim değerine dönüştürmek için 360° bakış açısıyla hareket eder. Güvenliğin yalnızca var olanı koruyan değil, yaşam alanının değerini ve güven duygusunu güçlendiren bir yapı olması için doğru analiz, doğru teknoloji ve doğru saha uygulamasını bir araya getirir. İLGİ Güvenlik, yaşam alanınızın ihtiyaçlarına uygun güvenlik mimarisi oluşturmak, riskleri önceden yönetmek ve güvenliği sürdürülebilir bir değere dönüştürmek için yanınızda. İhtiyaca özel analiz, doğru teknolojik kurgu, mevzuata uyumlu kayıt düzeni ve sahadaki operasyon disipliniyle güvenlik süreçlerinizi daha görünür, daha ölçülebilir ve daha yönetilebilir hale getirir. Bu bütüncül yaklaşım, günlük yaşam akışını kesintiye uğratmadan güven hissini güçlendirir; tesis yönetimine ise karar alırken dayanabileceği düzenli, anlaşılır ve izlenebilir bir güvenlik zemini sunar. Böylece güvenlik, yalnızca korunma değil, yaşam alanını değerli kılan sürekliliğin parçası haline gelir.



İLGi GÜVENLİK

360° Riskten Arınma Yaklaşımımız ile

modern yaşam alanlarının güvenlik standartlarını yeniden tanımlıyoruz.

Yasal mevzuata tam uyumlu veri kaydı ve proaktif yaklaşımlarımızla, yaşam alanınızın değerini ve güvenliğini en üst seviyede tutuyoruz.



Proaktif CCTV ve İzleme Sistemleri



Giriş-Çıkış ve Geçiş Kontrol Çözümleri



Kritik Nokta Alarm Sistemleri



Sistem Tasarımı ve Projelendirme



Entegre Çevre Güvenliği ve İhlal Tespiti



Veri Kaydı ve Arşivleme



ilgigrup.com

Güvenlik ve danışmanlık çözümleri **İLGi** gerektirir



@ilgigrup

Karayolu Taşımacılığında Güvenlik Önlemleri

Karayolu taşımacılığında güvenliği sağlayan en kritik unsurlardan biri, sürücünün dikkatli ve bilinçli hareket etmesidir. Sürücüler, trafik kazalarının önlenmesinde ve taşınan yüklerin güvenli bir şekilde hedefe ulaşmasında kilit rol oynar. Bu nedenle, sürücülerin eğitilmiş olması, yasal kurallara uyması ve dinlenme düzenine dikkat etmesi gerekir.

LEX LOJİSTİK

Karayolu taşımacılığı, global ticaretin ve yerel nakliye operasyonlarının en önemli taşıma türlerinden biridir.

Hem ağır yük taşımacılığı hem de günlük ihtiyaçların karşılanması, karayolu taşımacılığı önemli bir yer tutar. Ancak bu taşımacılık türünde güvenlik, taşımanın her aşamasında hayati bir rol oynar. Yüklerin güvenli bir şekilde varış

noktasına ulaşması, hem operasyonel süreçlerin sağlıklı işlemesi hem de can ve mal kaybının önlenmesi açısından kritik öneme sahiptir.

Güvenliğin ana bileşenleri:

Araç güvenliği: Araçların periyodik bakımlarının yapılması, güvenli taşımacılığın temel şartlarından biridir. Fren sistemi, lastik durumu, aydınlatma ve

sinyalizasyon sistemlerinin doğru çalışması, güvenli taşımacılık için olmazsa olmazlardır.

Sürücü güvenliği: Karayolu taşımacılığında sürücülerin tecrübesi ve dikkatli olması, kazaların önlenmesinde en önemli faktörlerden biridir. Sürücülerin yol güvenliği konusunda bilinçli olması, trafik kurallarına uyması ve düzenli aralıklarla dinlenmesi zorunludur.



“ Kritik tesisler, enerji santralleri, veri merkezleri, havaalanları, limanlar, askeri bölgeler ve akıllı şehir projeleri, güvenlik yatırımlarını yalnızca olay sonrası inceleme perspektifinden çıkararak proaktif tehdit yönetimi anlayışına taşıyor.

Yük güvenliği: Taşınan yüklerin doğru şekilde yerleştirilmesi, güvenlik tedbirleriyle sabitlenmesi ve taşınan yükün özelliklerine göre uygun araç seçimi yapılması, yük güvenliğini sağlamak için önemlidir.

Sürücü Güvenliği ve Dikkat Edilmesi Gerekenler

Karayolu taşımacılığında güvenliği sağlayan en kritik unsurlardan

biri, sürücünün dikkatli ve bilinçli hareket etmesidir. Sürücüler, trafik kazalarının önlenmesinde ve taşınan yüklerin güvenli bir şekilde hedefe ulaşmasında kilit rol oynar. Bu nedenle, sürücülerin eğitilmiş olması, yasal kurallara uyması ve dinlenme düzenine dikkat etmesi gerekir.

Sürücü güvenliğini artırmak için alınması gereken önlemler

Şunlardır:

Sürücü eğitimi: Karayolu taşımacılığı yapan sürücülerin profesyonel eğitimden geçmesi önemlidir. Trafik kuralları, uzun yol sürüş teknikleri ve kriz yönetimi konusunda eğitim alan sürücüler, daha güvenli sürüşler gerçekleştirir.

Dinlenme düzeni: Uzun yol sürüşlerinde sürücünün sürekli

araç kullanması dikkat dağınıklığı ve yorgunluk yapabilir. Avrupa Birliği'nde ve Türkiye'de yasal olarak belirlenmiş sürüş süreleri bulunmaktadır. Örneğin, sürücüler her 4.5 saatlik sürüşten sonra 45 dakikalık mola vermek zorundadır. Bu kurallara uymak, kaza riskini büyük ölçüde azaltır.

Trafik kurallarına uyum: Hız sınırlarına dikkat etmek, trafik işaret ve sinyallerini takip etmek, yoğun trafik durumlarında dikkatli davranmak, güvenli sürüşün temel ilkeleridir. Sürücüler, bu kurallara titizlikle uymalıdır.

Sağlık kontrolleri: Sürücüler, düzenli sağlık kontrollerinden geçmeli ve özellikle görme, işitme gibi sürüş güvenliğini etkileyen sağlık faktörlerinde problem olmadığından emin olmalıdır. Sürücünün sağlık durumu, güvenli sürüş için kritik bir öneme sahiptir.

Defansif sürüş: Sürücüler, diğer araçların hatalarını telafi edecek şekilde tedbirli sürüş tekniklerini öğrenmelidir. Tehlikeli durumlara karşı hazırlıklı olmak, potansiyel kazaların önlenmesinde önemli bir rol oynar. Sürücülerin bu tedbirlere uyması, karayolu taşımacılığında güvenliği artırır ve hem taşıdığı yüklerin hem de trafikteki diğer araçların güvenliğini sağlar.

Araç Güvenliği ve Düzenli Bakımın Önemi

Karayolu taşımacılığı sürecinde güvenliğin sağlanmasında en

önemli faktörlerden biri, taşıma aracının güvenilir durumda olması ve düzenli bakımının yapılmasıdır. Uzun mesafelerde taşımacılık yapan araçlar, yoğun kullanım ve zorlu yol koşullarına maruz kalır. Bu nedenle, araçların periyodik bakımları ve kontrolleri yapılmadan yola çıkılması, ciddi kazalara ve mal kaybına neden olabilir.

Araç güvenliği için dikkat edilmesi gereken başlıca unsurlar şunlardır:

Fren sistemi kontrolleri: Araç frenlerinin düzenli olarak kontrol edilmesi, güvenli taşımacılık için en kritik adımlardan biridir. Fren sistemindeki küçük bir aksaklık bile büyük kazalara yol açabilir. Özellikle ağır yük taşıyan araçlarda frenlerin performansı daha sık kontrol edilmelidir.

Lastik durumu: Lastiklerin yol tutuş kabiliyeti ve hava basıncı, taşımacılık sırasında güvenliği doğrudan etkiler. Eski, aşınmış veya patlama riski taşıyan lastikler kazaya neden olabilir. Araçların yola çıkmadan önce lastik basınçları kontrol edilmeli, gerekirse lastikler yenilenmelidir. Ayrıca, zorlu hava şartlarında kullanılan lastiklerin mevsim koşullarına uygun olması da önemlidir.

Aydınlatma ve sinyal sistemleri: Araç üzerindeki tüm aydınlatma ve sinyalizasyon sistemlerinin çalışır durumda olması gerekir. Özellikle gece sürüşlerinde farların ve stop lambaları

nın düzgün çalışması, sürücüye güvenli bir görüş sağlar ve diğer araçların da fark edilmesine yardımcı olur.

Süspansiyon ve direksiyon sistemleri: Araçların direksiyon sistemleri ve süspansiyonları da güvenli sürüş için düzenli olarak kontrol edilmelidir. Direksiyon sisteminde herhangi bir sorun, aracın kontrolünü zorlaştırabilir. Süspansiyon sistemi ise yol tutuşunu artırarak daha konforlu ve güvenli bir sürüş sağlar.

Araç yükleme kapasitelerine uyum: Araçların taşıyabileceği maksimum yük kapasitesine dikkat edilmelidir. Aşırı yüklenmiş araçlar, sürüş sırasında dengesizleşebilir ve kazalara yol açabilir. Ayrıca, yüklerin aracın içinde doğru şekilde yerleştirilmesi de önemlidir; yükler sabitlenmemişse ani frenlerde kayabilir ve dengeyi bozabilir.

Periyodik Bakım ve Kontrol Listesi: Taşıma araçlarının düzenli aralıklarla yetkili servislerde bakımdan geçirilmesi gerekir. Fren balataları, motor yağı, hava filtresi, lastiklerin durumu ve genel mekanik aksamların kontrolü, araç güvenliğinin sağlanmasında olmazsa olmazlardandır.

Araç güvenliğinin düzenli olarak sağlanması, hem taşınan yüklerin güvenli şekilde varış noktasına ulaşmasını sağlar hem de sürücü ve diğer yol kullanıcılarının güvenliğini korur.



Yük Güvenliği ve Doğru Yükleme Teknikleri

Karayolu taşımacılığında, taşınan yüklerin güvenli bir şekilde araç içinde sabitlenmesi ve doğru tekniklerle yerleştirilmesi hayati öneme sahiptir. Yanlış yükleme, dengesizlik, kayma, devrilme gibi riskler taşıyabilir ve hem sürücü hem de trafikteki diğer araçlar için ciddi tehlikeler oluşturabilir. Yük güvenliği, kazaların önlenmesi ve taşınan malların zarar görmekten teslim edilmesi açısından kritik bir unsurdur.

Yük güvenliğini sağlamak için dikkat edilmesi gereken başlıca unsurlar şunlardır:

Yüklerin Sabitlenmesi: Taşınan mallar, araç içinde uygun şekilde sabitlenmelidir. Yüklerin kaymasını veya devrilmesini engellemek için güvenlik halatları, gergi kayışları ve kilit mekanizmaları kullanılmalıdır. Özellikle ani frenlerde ve virajlarda yüklerin hareket etmesi tehlike oluşturabilir.

Ağırlık Dağılımının Dengeli

Yapılması: Yükleme sırasında, aracın ağırlık dağılımına dikkat edilmelidir. Ağırlığın aracın her iki tarafına eşit şekilde dağıtılması, sürüş sırasında aracın stabilitesini sağlar. Yüklerin bir tarafa fazla yüklenmesi, virajlarda dengesizliğe ve devrilme riskine yol açabilir.

Aşırı Yükleme Riskleri: Araçların taşıma kapasitesinin üzerine çıkılması, sadece aracın performansını düşürmekle kalmaz, aynı zamanda fren sistemleri üzerinde aşırı baskı oluşturur ve kazalara yol açabilir. Taşımacılık esnasında yasal sınırlar içerisinde kalmak, araç ve yol güvenliği açısından çok önemlidir. Her aracın maksimum taşıma kapasitesi belirlenmiş olup, bu sınırlara uyulmalıdır.

Malzeme Türüne Göre Yükleme:

Taşınan malzemenin türüne bağlı olarak farklı yükleme teknikleri kullanılmalıdır.

Kırılabılır veya hassas mallar için özel ambalajlar ve destekler kullanılarak, taşınan malların hasar görmesi önlenmelidir. Kimyasal maddeler veya tehlikeli malzemeler taşıyorsa, bu tür maddelerin güvenlik standartlarına uygun şekilde taşınması gerekir.

Yükleme ve Boşaltma Sırasında Alınacak Önlemler:

Yükleme ve boşaltma işlemleri sırasında, hem operatörlerin hem de taşımacılıkla ilgilenen personelin güvenliği sağlanmalıdır. Yükleme yapılan alanın düzenli ve uygun olması, kazaların önlenmesi açısından önemlidir. Ayrıca, yükleme sırasında kullanılan forklift, vinç gibi araçların da düzenli bakımları yapılmalı ve güvenli bir çalışma ortamı oluşturulmalıdır.

Yüklerin Araç İçi Dağılımı:

Yüklerin aracın içine dengeli bir şekilde dağıtılması gerekmektedir. Özellikle ağır yüklerin, aracın arka aksına doğru yerleştirilmesi, sürüş sırasında dengeyi artırır. Yüklerin birbirine yakın yerleştirilmesi, araçta hareket etmelerini engeller ve ağırlık merkezinin sabit kalmasına yardımcı olur.

Yük güvenliği, karayolu taşımacılığının en kritik aşamalarından biridir. Doğru tekniklerle yükleme yapılmaması, hem taşınan malların hasar görmesine hem de ciddi kazalara neden olabilir. Profesyonel lojistik firmaları, bu tür güvenlik risklerini minimize etmek için eğitimli personel ve doğru ekipmanlarla yükleme işlemlerini gerçekleştirir.

Ađır Y¼k TařımacılıĐında G¼venlik Önlemleri

Ađır y¼k tařımacılıĐı, lojistik sektöründe büyük bir öneme sahiptir. Özellikle sanayi, inřaat ve büyük ölçekli projelerde kullanılan ađır ve hacimli y¼klerin tařınması, bu alandaki en kritik ařamalardan biridir. Bu tür tařımacılık iřlemleri sırasında, olası kazaların ve zararların önüne geçmek için alınacak güvenlik önlemleri hayati bir rol oynar.

PUSAT LOJİSTİK



Ağır yük taşımacılığı, lojistik sektöründe büyük bir öneme sahiptir. Özellikle sanayi, inşaat ve büyük ölçekli projelerde kullanılan ağır ve hacimli yüklerin taşınması, bu alandaki en kritik aşamalardan biridir. Bu tür taşımacılık işlemleri sırasında, olası kazaların ve zararların önüne geçmek için alınacak güvenlik önlemleri hayati bir rol oynar. Pusat Lojistik olarak, yılların getirdiği tecrübe ve uzman kadromuzla, ağır yük taşımacılığında güvenliği en üst düzeyde sağlamayı hedefliyoruz. Ağır yük taşımacılığı sırasında yaşanabilecek olumsuz durumların önlenmesi, hem insan sağlığı hem de taşınan malların korunması açısından büyük önem taşır. Yanlış planlama, sistemsizlik ve yetersiz güvenlik önlemleri, ciddi kazalara ve maddi kayıplara yol açabilir. Bu sebeple, Pusat Lojistik olarak sektördeki en yüksek kalite ve güvenlik standartlarını benimseyerek, müşterilerimize güvenli ve sorunsuz bir taşımacılık hizmeti sunmayı taahhüt ediyoruz. Pusat Lojistik, ağır yük taşımacılığında karşılaşılan zorlukları ve riskleri minimize etmek için geniş araç filosu ve deneyimli ekibi ile Türkiye'nin dört bir yanına hizmet sunmaktadır. Güvenlik konusundaki hassasiyetimiz ve müşterilerimize sunduğumuz güven garantisi, sektördeki lider konumumuzu pekiştirmektedir. Bu makalede, ağır yük taşımacılığında karşılaşılan güvenlik risklerini ve bu risklerin nasıl yönetildiğini detaylı bir şekilde ele

alacağız. Ayrıca, Pusat Lojistik olarak benimsediğimiz güvenlik protokollerini ve müşterilerimize sunduğumuz hizmetleri sizlerle paylaşacağız. Böylece, ağır yük taşımacılığında güvenlik önlemlerinin ne denli önemli olduğunu bir kez daha vurgulamış olacağız.

Ağır Yük Taşımacılığında Karşılaşılan Güvenlik Riskleri

Ağır yük taşımacılığı, standart taşımacılık işlemlerine kıyasla daha yüksek riskler barındırır. Bu risklerin başında, taşınan yüklerin büyük ağırlığı ve hacmi gelir. Ağır yüklerin taşınması sırasında meydana gelebilecek kazalar, ciddi yaralanmalara veya maddi zararlara yol açabilir. Bu nedenle, güvenlik risklerini iyi anlamak ve bu risklere karşı önlem almak, başarılı bir taşımacılık sürecinin anahtarıdır.

Yüksek Ağırlık ve Hacimle İlgili Riskler

Ağır yük taşımacılığında, taşınan malzemelerin ağırlığı ve boyutları standart taşıma ekipmanları için uygun olmayabilir. Bu durum, taşıma sırasında araçlarda dengelessizliklere ve kontrol kaybına neden olabilir. Özellikle yükleme ve boşaltma süreçlerinde, yanlış yapılan işlemler yüklerin devrilmesine veya kaymasına yol açabilir. Bu tür olaylar, hem taşınan malzemenin zarar görmesine hem de personelin yaralanmasına sebep olabilir.

Taşıma Sırasında Oluşabilecek Kazalar ve Zararlar

Ağır yüklerin taşınması sırasında,

“ Ağır yük taşımacılığı sırasında yaşanabilecek olumsuz durumların önlenmesi, hem insan sağlığı hem de taşınan malların korunması açısından büyük önem taşır.

yol koşulları ve hava durumu gibi dış faktörler de riskleri artırabilir. Özellikle uzun mesafeli taşımacılıklarda, kötü hava koşulları veya kötü yol şartları nedeniyle araçların kontrolünü kaybetmesi muhtemeldir. Ayrıca, ani frenlemeler veya sert virajlar, yüklerin kaymasına ve araçların devrilmesine yol açabilir. Bu tür kazalar, hem taşınan malların zarar görmesine hem de trafik güvenliğinin tehlikeye girmesine neden olabilir.

Yanlış Planlama ve Sistemik Kaynaklı Riskler

Ağır yük taşımacılığında, detaylı bir planlama ve organizasyon eksikliği ciddi sorunlara yol açabilir. Yanlış yapılan zamanlama, rotaların iyi belirlenmemesi veya yeterli ekipmanın sağlanmaması gibi durumlar, taşımacılık sürecinin aksamasına ve beklenmedik problemlerin ortaya çıkmasına

“Acil durumlar için hazırladığımız planlar, taşıma sürecinde oluşabilecek beklenmedik durumlara karşı hazırlıklı olmamızı sağlar.

neden olabilir. Ayrıca, taşınacak yüklerin türüne uygun araçların ve ekipmanların seçilmemesi, yüklerin zarar görmesine ve taşıma işlemlerinin başarısız olmasına sebep olabilir. Bu riskler, ağır yük taşımacılığında güvenlik önlemlerinin önemini bir kez daha gözler önüne seriyor. Pusat Lojistik olarak, bu tür risklerin farkındayız ve her aşamada en yüksek güvenlik standartlarını uygulayarak, müşterilerimize güvenli ve sorunsuz bir hizmet sunmayı taahhüt ediyoruz.

Güvenlik Önlemleri ve Uygulamalar

Ağır yük taşımacılığında güvenliği sağlamak için alınacak önlemler ve bu önlemlerin doğru uygulanması hayati önem taşır. Pusat Lojistik olarak, bu önlemleri en üst düzeyde tutarak, taşıma sürecinin her aşamasında güvenliği sağlamaktayız. İşte ağır yük taşımacılığında alınması

gereken başlıca güvenlik önlemleri ve uygulamalar:

Doğru Yükleme ve Boşaltma Teknikleri

Yükleme ve boşaltma işlemleri, ağır yük taşımacılığının en kritik aşamalarından biridir. Bu aşamalarda yapılacak hatalar, ciddi kazalara ve yüklerin zarar görmesine yol açabilir. Doğru yükleme ve boşaltma tekniklerini kullanarak, yüklerin güvenli bir şekilde taşınmasını sağlıyoruz. Yüklerin dengeli bir şekilde yerleştirilmesi, kaymayı önleyici malzemelerin kullanılması ve uygun kaldırma ekipmanlarının seçilmesi gibi önlemler, bu sürecin güvenli bir şekilde tamamlanmasını sağlar.

Araç ve Ekipman Kontrolleri

Taşımacılık sırasında kullanılan araçların ve ekipmanların düzenli olarak kontrol edilmesi ve bakımlarının yapılması, güvenliği sağlamak için önemlidir. Araçların fren sistemleri, lastikleri, hidrolik sistemleri gibi kritik parçalarının düzenli olarak kontrol edilmesi ve bakımlarının yapılması, olası kazaların önüne geçer. Ayrıca, kullanılan kaldırma ve yükleme ekipmanlarının da periyodik olarak kontrol edilmesi ve gerektiğinde yenilenmesi, taşıma sürecinin sorunsuz ilerlemesini sağlar.

Personel Eğitimi ve Sertifikasyonu

Güvenli taşımacılık için, personelin eğitimi ve sertifikasyonu büyük önem taşır. Pusat Lojistik olarak, tüm personelimizi düzenli eğitimlerle bilinçlendiriyor ve

gerekli sertifikasyonları almalarını sağlıyoruz. Personelimiz, ağır yük taşımacılığı sırasında dikkat edilmesi gereken kurallar ve teknikler konusunda detaylı bilgi sahibidir. Bu sayede, taşıma sürecinde oluşabilecek riskleri minimize ediyor ve güvenliği en üst düzeyde tutuyoruz.

Güvenlik Protokollerinin Takibi

Taşımacılık sürecinde belirlenen güvenlik protokollerinin titizlikle takip edilmesi, güvenliği sağlamada kilit rol oynar. Pusat Lojistik olarak, taşıma sürecinin her aşamasında belirlediğimiz güvenlik protokollerine sıkı sıkıya bağlı kalıyoruz. Yüklerin taşıma- cağı rotaların belirlenmesi, yol ve hava durumu analizleri, acil durum planlarının hazırlanması gibi önlemlerle, olası risklere karşı her zaman hazırlıklı oluyoruz. Bu güvenlik önlemleri ve uygulamalar, ağır yük taşımacılığının güvenli ve sorunsuz bir şekilde gerçekleştirilmesini sağlar. Pusat Lojistik olarak, güvenlik konusundaki hassasiyetimizle, müşterilerimize her zaman en iyi hizmeti sunmayı amaçlıyoruz.

Pusat Lojistik'in Güvenlik Protokolleri

Pusat Lojistik olarak, ağır yük taşımacılığında güvenliği sağlamak amacıyla belirlediğimiz güvenlik protokolleri, sektördeki en yüksek standartları karşılamaktadır. Bu protokoller, taşıma sürecinin her aşamasında titizlikle uygulanmakta ve olası risklerin önüne geçilmektedir. İşte Pusat Lojistik'in benimsediği başlıca güvenlik protokolleri:

Güvenlik Standartları

Pusat Lojistik olarak, ulusal ve uluslararası güvenlik standartlarına uygun olarak çalışmaktayız. Taşıma süreçlerimizde, ISO 9001 ve OHSAS 18001 gibi kalite ve iş sağlığı ve güvenliği yönetim sistemlerini benimsemekteyiz. Bu standartlar, taşımacılık sırasında oluşabilecek risklerin minimize edilmesi ve sürekli iyileştirme prensibiyle güvenliğin en üst düzeyde tutulmasını sağlamaktadır.

Güvenlik Ekipmanlarının ve Teknolojilerinin Kullanımı

Güvenlik ekipmanlarının ve ileri teknolojilerin kullanımı, taşıma sürecinde güvenliğin sağlanmasında önemli bir rol oynar. Pusat Lojistik olarak, araçlarımızı ve ekipmanlarımızı en son teknolojilerle donatarak, taşıma sürecini daha güvenli hale getiriyoruz. GPS takip sistemleri, yük dengeleme sensörleri, güvenlik kameraları gibi teknolojiler sayesinde, taşıyan yüklerin her anını izleyebiliyor ve olası sorunlara anında müdahale edebiliyoruz.

Sürekli Eğitim ve Denetim Süreçleri

Personelimizin sürekli eğitimi ve denetim süreçleri, güvenlik protokollerinin etkin bir şekilde uygulanmasını sağlar. Pusat Lojistik olarak, tüm personelimizi düzenli eğitimlerle güncelleyerek, güvenlik konusunda bilinçli olmalarını sağlıyoruz. Ayrıca, taşıma süreçlerimizi



düzenli olarak denetleyerek, belirlediğimiz güvenlik protokollerine uyum sağlanmasını garanti altına alıyoruz. Bu denetimler, olası eksikliklerin tespit edilmesi ve hızlı bir şekilde giderilmesi açısından büyük önem taşır.

Acil Durum Planları

Acil durumlar için hazırladığımız planlar, taşıma sürecinde oluşabilecek beklenmedik durumlara karşı hazırlıklı olmamızı sağlar. Pusat Lojistik olarak, her taşıma işleminde acil durum planları oluşturarak, olası kazalara veya sorunlara karşı hızlı ve etkili bir şekilde müdahale edebiliyoruz. Bu planlar, personelimizin acil durumlarda nasıl hareket etmeleri gerektiğini belirler ve güvenliğini maksimum düzeyde tutar.

İşbirliği ve İletişim

Güvenlik protokollerinin etkin bir şekilde uygulanması, işbirliği ve iletişim ile sağlanır. Pusat Lojistik

olarak, müşterilerimizle sürekli iletişim halinde olarak, taşıma sürecinin her aşamasında bilgi akışını sağlıyoruz. Müşterilerimizin beklentilerini ve gereksinimlerini dikkate alarak, taşıma sürecini planlıyor ve gerekli güvenlik önlemlerini alıyoruz. Bu işbirliği, taşıma sürecinin sorunsuz ve güvenli bir şekilde tamamlanmasını sağlar.

Pusat Lojistik'in güvenlik protokolleri, ağır yük taşımacılığında güvenliği sağlamak ve müşterilerimize en iyi hizmeti sunmak amacıyla tasarlanmıştır. Bu protokoller sayesinde, taşıma sürecinde oluşabilecek riskleri minimize ediyor ve müşteri memnuniyetini en üst düzeyde tutuyoruz.

Müşteri Memnuniyeti ve Güvenliği Sağlama

Pusat Lojistik olarak, ağır yük taşımacılığında güvenliği sağlamak kadar müşteri memnuniyetine de büyük önem veriyoruz. Güvenlik

önlemlerimiz sayesinde müşterilerimize sunduğumuz hizmetin kalitesini artırıyor ve güvenli bir taşımacılık deneyimi sunuyoruz. İşte müşteri memnuniyetini ve güvenliğini sağlamak için benimsediğimiz bazı yaklaşımlar:

Müşterilere Sunulan Güvenlik Garantileri

Müşterilerimize, taşınacak yüklerin güvenliği konusunda tam bir garanti sunuyoruz. Bu garantiler, belirlediğimiz güvenlik protokollerine ve taşımacılık süreçlerimize duyduğumuz güvenin bir yansımasıdır. Müşterilerimize, taşınacak yüklerin her aşamada güvenli bir şekilde taşınacağını taahhüt ediyor ve olası risklere karşı her türlü önlemi aldığımızı belirtiyoruz. Bu güvence, müşterilerimizin bize olan güvenini pekiştiriyor ve uzun soluklu iş ilişkileri kurmamızı sağlıyor.

Güvenlik Önlemleri Sayesinde Sağlanan Müşteri Memnuniyeti

Güvenlik önlemlerimizin etkin bir şekilde uygulanması, müşterilerimizin memnuniyetini doğrudan etkiler. Güvenli bir taşımacılık hizmeti sunarak, müşterilerimizin taşınacak yüklerin zarar görmeyeceğinden emin olmalarını sağlıyoruz. Ayrıca, taşıma sürecinin her aşamasında müşterilerimize düzenli bilgilendirmeler yaparak, onların süreci takip etmelerine olanak tanıyoruz. Bu şeffaflık ve güvenlik odaklı yaklaşım, müşteri memnuniyetini artırır ve sadık müşteri kitlesi oluşturmamıza yardımcı olur.

Referanslar ve Başarı Hikayeleri

Pusat Lojistik olarak, bugüne

kadar gerçekleştirdiğimiz başarılı taşımacılık projeleri ve müşterilerimizden aldığımız olumlu geri bildirimler, güvenli hizmet anlayışımızın bir göstergesidir. Başarı hikayelerimiz ve referanslarımız, potansiyel müşterilerimize sunduğumuz hizmetin kalitesini ve güvenliğini kanıtlar niteliktedir. Bu başarılar, müşterilerimizin bize olan güvenini artırır ve yeni iş fırsatları yaratır.

Müşteri İletişimi ve Destek

Müşterilerimizle sürekli iletişim halinde olarak, onların taleplerini ve beklentilerini anlıyor ve bu doğrultuda çözümler üretiyoruz. Taşıma sürecinin her aşamasında müşterilerimize destek sağlayarak, olası sorunlara hızlı ve etkili bir şekilde müdahale ediyoruz. Ayrıca, müşteri memnuniyetini ölçmek için düzenli olarak geri bildirimler alıyor ve hizmet kalitemizi sürekli olarak iyileştiriyoruz. Pusat Lojistik olarak, müşteri memnuniyeti ve güvenliği sağlamak için benimsediğimiz bu yaklaşımlar, sektördeki lider konumumuzu pekiştirmektedir. Güvenlik odaklı hizmet anlayışımız ve müşteri memnuniyetine verdiğimiz önem sayesinde, müşterilerimizle uzun soluklu ve güvene dayalı iş ilişkileri kurmaktayız. Ağır yük taşımacılığı, lojistik sektörünün en zorlu alanlarından biridir ve güvenlik, bu süreçte en önemli unsurlardan biridir. Pusat Lojistik olarak, yılların deneyimi ve uzman kadromuzla, ağır yük taşımacılığında en yüksek güvenlik standartlarını benimsiyor ve müşterilerimize sorunsuz bir hizmet sunuyoruz.

Bu makalede, ağır yük taşımacılığında karşılaşılan güvenlik risklerini ve bu risklere karşı alınması gereken önlemleri detaylı bir şekilde ele aldık. Ayrıca, Pusat Lojistik olarak benimsediğimiz güvenlik protokollerini ve müşteri memnuniyetini sağlama konusundaki yaklaşımlarımızı paylaştık. Güvenlik önlemlerimiz, doğru yükleme ve boşaltma tekniklerinden, araç ve ekipman kontrollerine, personel eğitimlerinden, acil durum planlarına kadar geniş bir yelpazeyi kapsamaktadır. Bu önlemler sayesinde, taşıma sürecinde oluşabilecek riskleri minimize ediyor ve müşterilerimize güvenli bir taşımacılık deneyimi sunuyoruz.

Pusat Lojistik ile çalışmanın avantajları, sadece yüksek güvenlik standartları ile sınırlı değildir. Müşteri memnuniyetine verdiğimiz önem, sürekli iletişim ve destek sağlayarak, müşterilerimizin beklentilerini karşılamamızı ve aşmamızı sağlar. Başarı hikayelerimiz ve referanslarımız, sunduğumuz hizmetin kalitesini ve güvenliğini kanıtlar niteliktedir. Ağır yük taşımacılığında güvenliğini sağlamak ve müşteri memnuniyetini en üst düzeyde tutmak için, Pusat Lojistik olarak belirlediğimiz güvenlik protokollerine sıkı sıkıya bağlıyız. Güvenli ve sorunsuz bir taşımacılık hizmeti arıyorsanız, Pusat Lojistik sizin için doğru adres.

Bizimle iletişime geçerek detaylı bilgi alabilir ve teklif talebinde bulunabilirsiniz. Güvenli ağır yük taşımacılığı için Pusat Lojistik'i tercih edin ve taşımacılık süreçlerinizi güvenle bize emanet edin.

Yol Kullanıcılara Yönelik **Eğitimler**

GUVENLİ TRAFİK



Eğitim, insan davranışlarını istenen yönde değiştirme süreci olarak tanımlandığına göre insanlardan trafik güvenliği konusunda yapmalarını beklediğimiz davranışları onlara eğitim yolu ile kazandırmak çok daha önemli bir hale gelmiştir. Bu konudaki eğitim faaliyetleri hem örgün ve yaygın eğitim kurumlarında hem de motorlu taşıt sürücü kursları aracılığıyla yürütülmektedir.

Trafik kazalarının meydana gelmesinde en önemli unsurlardan biri yol kullanıcılarının davranışlarıdır. Yol kullanıcılarının davranışlarını, almış ve almakta oldukları eğitim ve daha önceki yolculuk deneyimleri

belirlemektedir. Trafik eğitimi sadece yol kullanıcı türü olarak tanımladığımız, sürücü, yaya, yolcu, bisikletli, motosikletliler değil; geleceğimiz olan çocuklarımızı, onları yetiştiren öğretmenleri, akademisyenleri, trafik denetimlerinden sorumlu birimleri, karayolu ulaşım altyapılarını tasarlayan ve inşa eden mühendisleri, politika yapımcıları kısacası bütün toplumu kapsamaktadır.

“Bütün yol kullanıcı türlerini kapayacak şekilde sürdürülebilir ve insan odaklı bir trafik eğitimi, trafik kazalarının azalması için en etkili enstrümanlardan biri olarak tanımlanabilir.” Trafikte bilinç ve sorumluluk; trafik eğitimi ile bireye ne kadar erken yaşlarda kazandı-

rılırsa, sonuç da o denli etkili olmaktadır. Küçük yaşlarda trafik konusunda eğitim alan çocuklar, günümüz trafiğinde kendilerini korudukları gibi geleceğin sorumluluk sahibi yetişkin yaya ve sürücüleri olarak toplumun özünü oluşturacaklardır.

Trafik ve yol güvenliği eğitimi; okul öncesinden başlamak suretiyle yol kullanıcısı olarak devam eden (sürücü, yolcu, yaya) yaşam boyunca sürdürülebilir bir biçimde sağlanmalıdır. Yaşam boyunca sürdürülebilir bir eğitim politikası, yol kullanıcılarının, yol güvenliğinin neden bu denli önemli olduğunu ve belli bazı tedbirleri anlayabilmelerini sağlayacaktır.

İçişleri Bakanlığı Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığı tarafından; Trafik Dedektifleri, Hatalı Sürücüye Kırmızı Döğük, Yaya Öncelikli Trafik, Yaşam Tüneli, İyi Dersler Şoför Amca, Simülasyon Aracı, Mobil Trafik Eğitim Tırı, Mobil Trafik Eğitim Aracı ve benzeri projeli eğitim faaliyetleri sonucunda başta çocuklar ve öğrenciler olmak üzere binlerle ifade edilebilen yol kullanıcılarına trafik güvenliği konusunda eğitimler vermeye devam edilmektedir.



Avrupa'da özellikle 90'lı yılların sonu ve 2000'li yılların başında meydana gelen Mont Blanc (Fransa-İtalya) ve Tauern (Avusturya-İtalya) tünel felaketleri (1999) ve Gotthard (İsviçre-İtalya) tüneli yangını (2001) gibi art arda meydana gelen felaketler tünel güvenliği konusunda ilgiyi artırmıştır.

KARAYOLLARI GENEL MÜDÜRLÜĞÜ

Karayolları Genel Müdürlüğü kurulduğu günden bu yana öncü bir kuruluş olarak, ülkemize birçok teknolojik yeniliği ve gelişmeyi kazandırmış ve üstlendiği görevin gereği birçok önemli mühendislik yapısını başarıyla projelendirmiş, yapımını tamamlayarak, hizmete sunmuştur. Ülkemiz karayolu ulaşımını

yüksek standartlara ulaştırmak hedefiyle sürdürdüğümüz çalışmalarımızda seyahat konforu, milli ekonomiye katkı, diğer ulaşım sektörleriyle uyumlu ulaşım sistemi tesis etmenin yanında, göz önünde bulundurduğumuz en önemli hususların başında güvenlik gelmektedir. Karayolu ulaşımının gelişim çizgisi incelendiğinde, yollar ve üzerindeki tüm sanat yapıları-

nın, farklı uzmanlık alanlarının bir araya gelmesiyle tesis edilen modern birer mühendislik eseri olduğu ve tüm sektörlerin altyapısındaki önemi ve gelişim hızıyla pek çok yeniliği de beraberinde getiren teknolojinin, tüm projelere damgasını vurduğu bir dönem yaşanmaktadır. Bu sürecin etkisini gösterdiği alanlardan biri de güvenlik önlemleri olmuş, tünel güvenliği

“ Karayolları Genel Müdürlüğü 2005 yılında kurmuş olduğu bir komisyonla 2004/54/EC sayılı karara uygun olarak çalışmalar başlatmıştır. Özellikle tünellerde ağır yük taşımacılığı ve tehlikeli madde taşımacılığına yönelik risk analizi çalışmaları yapılmıştır.

konusunda yaşanan gelişmeler, ülkemizdeki tünellerin kontrol ve yönetiminde yerini almıştır. Ülkemizdeki tünelcilik çalışmalarını genel olarak incelediğimizde; özellikle ticaret hacminin artarak, limanlarımızın daha teknik ve verimli kullanılmasını ve bu limanların ülkemiz içerisinde birbirleriyle karayolu ulaşım bağlantısının sağlanmasını zorunlu hale getirdiği iki binli yıllarda, tünel yapım çalışmalarının ivme kazandığı görülmektedir.

Avrupa'dan gelen yükler Rusya'ya, Kafkasya'ya, Orta Asya ülkelerine Karadeniz limanları aracılığıyla, aynı şekilde Ortadoğu, Afrika, Güney Avrupa

ve okyanus aşırı olan ticaretimiz de Akdeniz limanlarımızdan yapılmaktadır. Bu limanlara gelen mal ve yüklerin ülke içerisindeki belirli merkezlere taşınması ihtiyacı ortaya çıkmış, kuzey-güney akslarımızın iyileştirilmesinin gerekliliği ve önceliği gündeme gelmiştir. Bu çalışmanın doğal sonucu olarak birçok tünel yatırımı hayata geçirilmiştir. Tünellerin varlığı fırsatları artırırken, bölgesel, ulusal ve uluslararası ilişkilerin gelişimi ve izole gibi görünen bölgelerin ekonomik refahı için katalizör olmuştur.

2003-2018 yılları arasında 413 km uzunluğunda 278 adet tünel yapılmış olup bugün itibarıyla tüm yollarımızda toplam 463 km uzunluğunda 361 adet tünel hizmet vermektedir. Bu dönemde gerçekleştirilen çalışmalarla kaydedilen tünel uzunluğu artışı yüzde 826 olmuştur. 2023 yılına kadar yol ağıımızda toplam 700 km uzunluğunda 470 adet tünelin trafiğe hizmet vermesi hedeflenmektedir. Karayolu ulaşımı için zor ve karmaşık bir jeolojik yapısı olan ülkemizde son yıllarda tünelcilik sektöründe yaşanan başarımlı gelişmeler, tünelcilik alanında geçmişten bugüne elde edilen tecrübe kazanımlarının en yeni teknoloji ürünleri kullanılarak sürdürülen imalatlarla desteklenmesi, hem ulusal hem uluslararası alanda teknik anlamda ileri bir seviyede yer almamızı sağlamıştır.

Ülkemizdeki tünel sayısının önemli ölçüde artması, 10 kilometreden uzun tünellerin

yapımına başlanması, tünel güvenliği konusundaki çalışmaların önemini de artırmıştır. Karayolu tünellerinde güvenlik kriterlerinin sağlanması, mevcut tünellerin eksiklerinin belirlenip bu kriterler doğrultusunda gerekli tedbirlerin alınması, yapılması planlanan tünellerin her aşamasında göz önünde bulundurulması tünel güvenliğinin sağlanmasında önemli hale gelmiştir.

Tünel güvenliği çalışmalarının tarihçesi ve ülkemizde yapılan çalışmalar

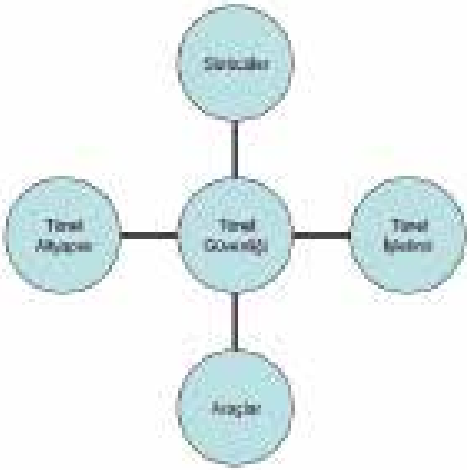
Avrupa'da özellikle 90'lı yılların sonu ve 2000'li yılların başında meydana gelen Mont Blanc (Fransa-İtalya) ve Tauern (Avusturya-İtalya) tünel felaketleri (1999) ve Gotthard (İsviçre-İtalya) tüneli yangını (2001) gibi art arda meydana gelen felaketler tünel güvenliği konusunda ilgiyi artırmıştır.



Resim 1. Gotthard Tüneli Yangını

2001 yılında, AB Ortak Ulaştırma Politikası kapsamına alınan tünel güvenliği konusunda AB komisyonu yıllar süren istişarelerden sonra 2004 yılında, 2004/54/EC sayılı karayolu tünellerinde yapısal, teknik ve işletmeye yönelik bir dizi uyumlaştırılmış asgari güvenlik stan-

dartlarını ortaya koymuştur. Bu çalışmada bütünsel yaklaşım kabul edilmiş ve tünel güvenliği 4 ana başlığın içerisinde değerlendirilmiştir.



Resim 2. 2004/54/EC'ye göre bütünsel olarak değerlendirilen başlıklar

Karayolları Genel Müdürlüğü gelişmeleri yakından takip ederek 2005 yılında kurmuş olduğu bir komisyonla 2004/54/EC sayılı karara uygun olarak çalışmalar başlatmıştır. Tünel güvenlik kriterlerine uygun yapım şartnameleri hazırlanmış, tünellerin işletme ve yönetim sistemi planlanmış, sürücülerin bilinçlendirilmesi amaçlı bildiriler yayınlanmış ve özellikle tünellerde ağır yük taşımacılığı ve tehlikeli madde taşımacılığına yönelik risk analizi çalışmaları yapılmıştır. Yapılan çalışmalar aşağıda listelenmiştir.

1- 2005 yılında 2004/54/EC'ye uygun tünellerin yapımına yönelik minimum güvenlik kriterlerinin belirlenmesi ve

şartnamelerin buna göre düzenlenmesi

2- 2007 yılından itibaren Karayolları Genel Müdürlüğü olarak tünellerin yapım ve işletmesine yönelik, teşkilat yapılanmasında birimler oluşturulması, bölgesel olarak da Tünel Bakım Onarım İşletme Şefliklerinin kurulması

3- 2013 yılından itibaren tünellerde, ulusal ve uluslararası mevzuatlara uygun Tehlikeli Madde Taşımacılığı konusunda risk analizi çalışmaları yapılma-ya başlanması,

4- 2015 yılında Tünel İşletme Yönetmeliğinin çıkarılması

5- Tünel ekipmanları ve tünel güvenliğine yönelik; envanter tutulması, tünellerin coğrafi bilgi sistemlerinde gösterimi, sorgulanması, kaza envanterlerinin ve kayıtlarının tutulması amaçlı Tünel Bilgi Sistemi Programı çalışmaları yapılması

6- Mevcut tünel sistemlerinde kullanılan bütün ekipmanların, yazılım ve sistemlerin tek bir yazılım üzerinden izlenebildiği, yönetilebildiği bir sistemin kurulması ve Karayolları Tünel Altyapı Sistemleri Kontrol ve İzleme Sistemi Yazılımının oluşturulmasına yönelik çalışmalar yapılması

7- Tünel kullanıcılarına yönelik bilgilendirme ve tünel güvenliği konusunda farkındalık oluşturma çalışmaları yapılması

8- Tünelere acil müdahale konusunda diğer kurumlarla işbirliği yapılarak, tatbikatlar düzenlenmesi ve acil durum senaryolarının hazırlanması, **9-** Tünel güvenliği konusunda

“Tünellerde meydana gelen kaza, yangın vb. olaylar, açık yoldaki benzer kazalara göre daha az yaşanmakla birlikte bireysel, toplumsal ve ekonomik riskler yönünden çok daha vahim sonuçlar doğurmaktadır.

ulusal ve uluslararası akademik çalışmaların desteklenmesi ve takibi

Çalışmalarda gelinecek durumlar ve kısa vadede hedefler

Konuya ilişkin tüm yenilikler takip edilmekte ve tünel yapım şartnamelerinin güncelliğini koruması sağlanmaktadır. Tünellerin yapısal özelliklerinin yanında güvenliği için kullanılan elektromekanik sistemler ana başlıklar halinde aşağıda sıralanmıştır.

- ▮ SCADA (Uzaktan İzleme ve Gözetleme Sistemleri)
- ▮ Havalandırma Sistemleri (Normal ve Acil Durum Havalandırma Otomasyonları)



GÜVENLİKTEDARİK.com

Son teknolojiye uygun, ürün ve çözümlerden **HABERİNİZ VAR MI?**

- Elektrik proje taahhüt firmaları • Bayi odaklı çalışan firmalar
- Havalimanları ilgili birimleri • Bankalar ilgili birimleri • İnşaat firmaları
- Oteller ilgili birimleri • Hastaneler ilgili birimleri • AVM'ler ilgili birimleri
- TÜRKLİM Üyeleri • Belediyeler ilgili birimleri • Emniyet Genel Müdürlüğü ilgili birimleri • Zincir mağazalar • Üniversiteler • Mimarlık ofisleri
- Sektör profesyonelleri **AĞIMIZA KATILIN**

TÜM TÜRKİYE'DE SESİNİZ OLALIM!

- ✓ CCTV ve video kontrol sistemleri,
- ✓ Yangın algılama ve ihbar sistemleri,
- ✓ Yangın söndürme sistemleri,
- ✓ Geçiş kontrol sistemleri,
- ✓ Hırsız alarm sistemleri,
- ✓ Alarm izleme merkezleri,
- ✓ Apartman konuşma sistemleri,
- ✓ Mobil takip sistemleri,
- ✓ Drone teknolojileri

Çok sayıda farklı firmamızın çözüm ortağı olarak ve geleceği tasarlarken bir arada çalışarak hizmet ağına olan **GÜVENLİK YÖNETİMİ** tarafından gerçekleştirilmektedir. Başta olmak üzere GÜVENLİK YÖNETİMİ, PERPA GÜVENLİK, TECHNEWS ve KURUMSAL YATIRIMCI dergileri tarafından **ARKHO TANIYIM HİZMETLERİ** gibi tasarım, kurulum ve bakım çözümleri, web ve her türlü promasyon ihtiyaçlarına farklı yollarla tasarımı, hazırlama ve müşteriye konuyla ilgili bilgilendirme çözümleri sunulmaktadır.

Güvenlik Yönetimi
GÜVENLİK YÖNETİMİ

arkho
TANIYIM HİZMETLERİ

www.guvenlikyonetimi.com

- Aydınlatma Sistemleri (Kademeli Aydınlatma)
- Yangın Algılama ve Önleme Sistemleri
- Trafik Güvenliği Sistemleri (Trafik Mesaj Sistemleri, Trafik İşaretleme Sistemleri, Hız Algılama, Plaka Tanıma, Kamu Anons Sistemi, Buz Önleme Sistemi vb)
- Kamera Sistemleri,
- Enerji Sistemleri vb.

Karayolları Genel Müdürlüğü teşkilat yapısında, mevcut yapının tünel işletme şefliklerine odaklandığı çözümler geliştirilmektedir. Bunun yanında Karayolları Genel Müdürlüğü,

“ Tünel altyapı sistemlerinin birleştirilmesine yönelik çalışma kapsamında, tüneller arasında fiber optik altyapıdaki eksikliklerin giderilmesi ve ortak yazılım geliştirilmesine yönelik çalışmalar devam etmektedir. ”

Tehlikeli Mal ve Kombine Taşımacılık Düzenleme Genel Müdürlüğü ve AFAD koordinasyonunda tünel güvenliği ile ilgili çalışma grupları oluşturulmuş olup, trafik güvenliği konusunda mevzuatları düzenlemeye yönelik çalışmalar devam etmektedir.

Tünellerde tehlikeli madde taşımacılığı: Tüneller, genel olarak engebeli alanları aşmak ve şehirlerdeki trafik sıkışıklığını rahatlatmak için kullanılmakta olup, tehlikeli madde yüklü ağır vasıtaları, tünel yerine standardı düşük dağlık yollara, şehir merkezinden geçen yoğun



trafiğe ya da sahil yollarına yönlendirmek daha yüksek çevresel ve toplumsal risklere neden olabilmektedir. Bu nedenle karar aşamasında tehlikeli maddelerin tünelden geçirilmesiyle ilgili oluşabilecek risk, alternatif rotalarda yapılacak taşımaya bağlı risklerle karşılaştırarak en uygun çözüm üretilmektedir. Risk analizi konusunda uluslararası kabul gören QRAM (Quantitative Risk Analyse Methodology) yaklaşımıyla tüm tünellerimizde, alternatif güzergahlarıyla beraber ADR (Tehlikeli Maddelerin Karayolu ile Taşınmasına İlişkin Avrupa Anlaşması)'ye ve 'Tehlikeli Maddelerin Karayolu ile Taşınmasına Hakkında Yönetmelik'e uygun olarak çalışılmış ve taslak çalışma tamamlanmıştır. 2019 yılı sonuna kadar hangi tünellerimizden hangi koşullarda, hangi tanımlı malzemelerin geçeceği ve geçişte uygulanacak kuralların tamamlanması hedeflenmektedir. Diğer taraftan, Ulaştırma ve Altyapı Bakanlığı bünyesinde; karayolu, demiryolu ve denizyolu tehlikeli madde taşımacılığını düzenleyecek, özellikle de tehlikeli madde taşımacılığını karayolu yerine ana akslarda demiryolları, sahil kesiminde ise denizyolu ile sağlamaya yönelik çalışmalar da 2019 itibarıyla başlamıştır. Tünel Bilgi Sistemi Programı çalışmalarının envantere dayalı büyük bir kısmı tamamlanmış olup, tünel güvenliğine yönelik katkılarla yazılım güncellenmektedir.

“Tünel altyapı sistemlerinin birleştirilmesine yönelik çalışma kapsamında, tüneller arasında fiber optik altyapıdaki eksikliklerin giderilmesi ve ortak yazılım geliştirilmesine yönelik çalışmalar devam etmektedir.

Tünel altyapı sistemlerinin birleştirilmesine yönelik çalışma kapsamında, tüneller arasında fiber optik altyapıdaki eksikliklerin giderilmesi ve ortak yazılım geliştirilmesine yönelik çalışmalar devam etmektedir. Bu çalışmanın tamamlanması tüm tünellerin tek bir noktadan izlenebilmesi ve olası kaza, yangın vb. durumunda, yönetimin tek bir noktadan sağlanması açısından önemlidir. Tünelere acil durum müdahalesi çalışmaları, tünellerin bulunduğu bölgelerdeki kolluk kuvvetleri, itfaiye, ambulans ve tünel işletmecileri arasında koordinasyonun sağlanmasına yönelik Valiliklerin de devreye girdiği bölgesel bazlı çalışma grupları üzerinden devam etmektedir. Tünel kullanıcıları ve araçların tünel güvenliğine etkisi konusunda farkındalık oluşturulmasına yönelik çalışmalar devam etmekte olup, özellikle sürücü ve araçların tünel güvenliğine etkileri konusunda akademik çalışmalara ihtiyaç duyulmaktadır.

Sonuç

Tünellerde meydana gelen kaza, yangın vb. olaylar, açık yoldaki benzer kazalara göre daha az yaşanmakla birlikte bireysel, toplumsal ve ekonomik riskler yönünden çok daha vahim sonuçlar doğurmaktadır. Söz konusu tünel kazalarının doğrudan etkilerinin yanı sıra, tünellerin uzun süre kapalı kalması sebebiyle, alternatif güzergâhlarda trafik sıkışıklığına yol açması da kaza oranlarını yükseltmektedir. Yukarıda bahsedilen Gotthard Tüneli yangını sonucu tünelin kapanması nedeniyle İtalya ekonomisi 2,5 milyar Euro zarara uğramıştır. Tüm Avrupa ekonomisine zararın 15 milyar Euro'yu bulduğu tahmin edilmektedir. Sonuç olarak karayollarında tünel güvenliği konusunda 4 ana başlıktan oluşan bütünsel yaklaşım çerçevesinde bundan sonra da hem kurumsal, hem akademik hem de toplumsal farkındalık sağlanması ve konunun kamuoyu önünde de güncel tutulması gerekmektedir.



Avrasya Tüneli'nde bütüncül güvenlik önlemleri

Tünel içinde ve yaklaşım yollarında bulunan yaklaşık 400 kamera ile beslenen SCADA kontrol ve takip sistemi tünelin her noktasına hakimdir. Otomatik olay algılama sistemi, duran araç, yaya, duman ve düşen obje gibi olağandışı bütün olayları tespit edebilmekte ve daha önce tanımlı olan 26 adet senaryodan uygun olanını en kısa sürede aktive etmektedir.

AVRASYA TÜNELİ

İstanbul trafiğinin en yoğun olduğu Kumkapı-Koşuyolu semtleri arasındaki yolculuk süresini 5 dakikaya indiren Avrasya Tüneli, derinliği ve büyüklüğü ile daha önce hiç denenmemiş bir başyapıt olarak milimetrik hesaplarla inşa edilmiş bir yapıdır.

Projenin inşasından işletmesine kadar tüm süreçlerde güvenlik ilk öncelik olarak konumlandırılmıştır. İnşaat ve işletme aşamalarında

daima en ileri ve en güncel teknolojileri kullanan Yapı Merkezi ve SK E&C'nin dünyanın her noktasında kazandığı deneyim, Avrasya Tüneli'nin en önemli teknik güvencesini oluşturmaktadır.

En yenilikçi teknolojiler ile güvenlik

Deniz suyuyla temas etmeyen tünelin yapımında ileri teknoloji ürünü tünel açma makinesi TBM kullanı-

mıştır. 127 yıllık tasarım ömrüne sahip beton bloklardan oluşan tünelin inşa sürecinde 0 tolerans üzerine kurulu binlerce test yapılmış, tünel güvenliği için en yenilikçi teknolojiler kullanılmıştır. Tünel, yangından zarar görmeyecek ve su sızdırmayacak şekilde tasarlanmıştır. Ayrıca tünelde atık suların dışarı çıkarılması için yüksek kapasiteli bir drenaj sistemi bulunmaktadır.

İstanbul'un, Kuzey Anadolu Fay

Hattı'nın tam üzerinde olması dolayısıyla Avrasya Tüneli'nin güzergah belirlenmesi ve tasarımı da buna göre yapılmıştır. Proje, fay sisteminin üretebileceği en büyük depreme dayanıklı olarak inşa edilmiştir. Tünelde yer değiştirmeleri en aza indirmek üzere Japonya'da imal edilen iki sismik bilezik bulunmaktadır. Bu sayede tünel doğaya karşı direnç göstermemekte, harekete müsaade etmektedir. Tünelin inşa sürecinde binlerce çalışana her vardiyada verilen onbinlerce saatlik eğitimlerin karşılığını hiçbir büyük iş kazası ve can kaybı yaşamamasıyla alan Avrasya Tüneli, aynı titizliği tüneli kullanan yolcuları için de göstermektedir.

Avrasya Tüneli, Asya Yakası'nda elektrik kesintisi durumunda Avrupa Yakası'ndan, Avrupa Yakası'nda elektrik kesilmesi durumundan Asya Yakası'ndan enerji sağlamakta; şehir genelinde bir kesinti olması durumunda güçlü UPS ve jeneratör sistemi devreye girmektedir.

400 kamera ile beslenen takip sistemi

Tünel içinde ve yaklaşım yollarında bulunan yaklaşık 400 kamera ile beslenen SCADA kontrol ve takip sistemi tünelin her noktasına hakimdir. Otomatik olay algılama sistemi, duran araç, yaya, duman ve düşen obje gibi olağandışı bütün olayları tespit edebilmekte ve daha önce tanımlı olan 26 adet senaryodan uygun olanını en kısa sürede aktive etmektedir. Bu çerçevede tünel otomatik olarak kapatabilmekte, havalandırma sistemleri, VMS, radyo anonsları otomatik olarak çalışmaktadır. Tünelde buna ek olarak doğrusal yangın algılama sistemi, 1000'in üzerinde yangın alarm noktası (duman detektörü, yangın ihbar butonu vb.) ve 100 adet acil telefon bağlantısı bulunmaktadır. Tünelde, acil durum telefonları, kamu

anons sistemi, radyo anonsu ve GSM alt yapısı sayesinde yolculuk esnasında kesintisiz bir iletişim imkânı sağlanmakta ve acil durumlarda bilgi akışı sağlanabilmektedir. En derin noktası deniz seviyesinin 106 metre altından geçerek Avrupa ve Asya'yı birbirine bağlayan Avrasya Tüneli'nden alınan görüntüler kontrol merkezindeki görüntüleme ekranlarına yansıtılmakta ve her an denetlenmektedir. Tünel girişlerinde ve içerisinde 7/24 görev yapan her türlü donanım ve eğitime sahip ilk müdahale ekipleri, herhangi bir olaya en geç 2 dakika içerisinde müdahale ederek sürücülere destek vermektedir. Avrasya Tüneli'nin fiziki yapısı ve ihtiyaçları için özel olarak tasarlanan ilk müdahale araçları, her türlü kazaya anında müdahale edebilecek şekilde teçhizatlandırılmıştır. Tünelin her iki katında belirlenmiş olan noktalarda hazır bulunan motorlu acil müdahale araçları kamera kayıtlarını izleyen ekip tarafından olay yerine yönlendirilmektedir. Avrasya Tüneli için özel olarak üretilen motorlu araçlar yangın söndürme aparatlarına kadar tam teşekkülle donatılırken, uzman personel; ilkyardımdan ileri sürüş tekniklerine, iletişimden stres yönetimine kadar onlarca periyodik eğitimleri başarı ile tamamlayan kişilerden oluşmaktadır. Kullanıcıları için güvenlikle ilgili her konunun tüm detaylarıyla düşünüldüğü Avrasya Tüneli'nde gün ışığına en yakın olan ve seyahat boyunca göz yormayan LED aydınlatma teknolojisi kullanılmıştır.

Yangın anında tesbit edilebiliyor

Tünel, yapısal olarak pasif yangın koruma, işletme teknolojisi olarak ise yangın algılama ve söndürme sistemleri ile korunmaktadır. Olası bir

yangın, anında tespit edilmektedir. Her 200 metrede bir yer alan, alt ve üst katlar arasında geçişi sağlayan sızdırmazlık özelliğine sahip odalar, acil durumlarda güvenli kata tahliye için uygun olarak tasarlanmıştır. Tünel içinde bulunan ve çift yönlü çalışabilen 92 adet jet fan yoğun trafik ve yangın durumunda kirli havayı büyük bir hızla tahliye edebilmekte ve sürekli temiz hava sağlamaktadır. Tünelde 7/24 görevli acil müdahale ekipleri; AFAD, İstanbul İtfaiyesi, 112 Ambulans ve Emniyet Genel Müdürlüğü gibi hizmet birimleri ile kesintisiz koordinasyon sağlamaktadır. Her 600 metrede bir konumlanan araç bekleme cepleri acil durumlarda hem sürücülere hem de müdahale ekiplerine duraklama imkanı tanımaktadır.

Asya ve Avrupa yakaları arasında en hızlı ulaşım olanağını sağlayan Avrasya Tüneli'nde güvenliğin kusursuz şekilde sağlanması amacıyla çok kapsamlı ve bütüncül yapıda güvenlik önlemleri alınmıştır. Bu doğrultuda tünelde güvenlik için 2.8 m yükseklik, 5 ton ağırlık ve 70 km hız sınırı bulunmaktadır. Tünel, kamyon, motosiklet, bisiklet ve yayaalara kapalıdır. Sürücülerden tünele girmeden önce yakıt seviyelerini kontrol etmeleri, güneş gözlüklerini çıkarmaları, cep telefonu kullanmalarını, farları ile radyolarını açmaları ve tünel güzergahı boyunca tüm trafik işaretlerini takip etmeleri rica edilmektedir.

İleri teknoloji sistemleri ile emniyetli ve konforlu bir yolculuk imkanı sağlayan Avrasya Tüneli'nin bu titiz çalışmaları açıldığı günden bu yana uluslararası saygınlığa sahip kurum ve kuruluşlar tarafından 11 ödülle taçlandırılmıştır. 2018 yılında 17.6 milyon aracı karşı kıtaya ulaştıran Avrasya Tüneli'nde güvenlik ilk öncelik olmaya devam edecektir.

2026 hemşire çağrı sistemleri pazarı

Modern hastanelerde güvenlik yalnızca bina girişlerini kontrol etmekten ibaret değildir. Hastanın yatağından yaptığı tek bir çağrı, yoğun bakımda saniyeler içinde verilen bir alarm ya da sağlık çalışanının maruz kaldığı şiddet sırasında bastığı panik butonu, doğrudan insan hayatını etkileyen kritik güvenlik süreçlerinin başlangıcıdır. Günümüzün IP tabanlı hemşire çağrı sistemleri; hasta güvenliği, personel güvenliği ve acil durum yönetimini tek bir platformda buluşturarak sağlık tesislerinin vazgeçilmez altyapılarından biri haline gelmiştir.

DERLEME: DERYA BOZKURT



Sağlık sektörü son yirmi yılda tarihinin en büyük dijital dönüşümünü yaşamaktadır. Tanı ve tedavi teknolojilerindeki gelişmeler, robotik cerrahi sistemleri, yapay zekâ destekli görüntüleme çözümleri ve elektronik sağlık kayıtları hastanelerin çalışma biçimini kökten değiştirmiştir. Ancak bu dönüşümün görece daha az konuşulan, fakat hasta güvenliği açısından en kritik bileşenlerinden biri de hemşire çağrı sistemleridir.

Geçmişte hemşire çağrı sistemleri, hasta yatağının yanında bulunan basit bir buton ve hemşire bankosunda yanan bir lambadan ibaret görülüyordu. Hastanın düğmeye basmasıyla birlikte koridordaki ikaz lambası yanıyor, hemşire odanın numarasını görerek hastaya ulaşıyordu. Döneminin ihtiyaçlarını karşılayan bu sistemler, hastanelerin büyümesi, servislerin karmaşıklaşması ve sağlık hizmetlerinin çeşitlenmesiyle birlikte yetersiz kalmaya başladı.

Bugün yüzlerce yatağa sahip büyük şehir hastaneleri, üniversite hastaneleri ve özel sağlık kampüsleri, aynı anda binlerce hastaya hizmet vermektedir. Bu ölçekte hizmet veren yapılarda iletişimin yalnızca görsel ikaz lambalarıyla yürütülmesi artık mümkün değildir. Bir hastanın yardım çağrısının doğru kişiye, doğru öncelik ve mümkün olan en kısa sürede ulaştırılması hayati önem taşımaktadır. Aynı şekilde sağlık çalışanlarının güvenliği, acil kod uygulamaları ve hastane içerisindeki iş akışlarının yönetimi de çağrı sistemlerinin kapsamına

girmiştir.

Bu nedenle hemşire çağrı sistemleri artık yalnızca hasta ile hemşire arasında iletişim sağlayan teknolojiler olarak değil, hastanenin dijital iletişim omurgası olarak değerlendirilmektedir. Günümüzde gelişmiş sistemler yalnızca çağrıyı iletmekle kalmakta, çağrının önceliğini belirlemekte, ilgili personeli otomatik olarak yönlendirmekte, müdahale sürelerini kayıt altına almakta ve hastane yönetimine ayrıntılı performans raporları sunmaktadır. Sağlık hizmetlerinde zaman çoğu zaman tedavinin bir parçasıdır. Kalp krizi geçiren bir hastaya dakikalar içinde müdahale edilmesi ile on dakika sonra müdahale edilmesi arasında yaşamı belirleyen büyük bir fark bulunmaktadır. Aynı şekilde yaşlı bir hastanın banyoda düşmesi sonrasında yardım gelene kadar geçen süre de oluşabilecek komplikasyonların şiddetini doğrudan etkileyebilir. Bu nedenle hemşire çağrı sistemleri yalnızca iletişim altyapısı değil, aynı zamanda hasta güvenliği stratejilerinin temel bileşenlerinden biridir.

Dünya genelinde sağlık hizmetlerinin dijitalleşmesiyle birlikte hemşire çağrı sistemlerinin fonksiyonları da büyük ölçüde değişmiştir. Artık bu sistemler kamera sistemlerinden bina otomasyonuna, yangın algılama altyapısından hastane bilgi yönetim sistemlerine kadar birçok teknolojiyle entegre çalışmaktadır. Böylece hastane içerisindeki farklı disiplinler arasında gerçek zamanlı bilgi paylaşımı mümkün hale gelmektedir. Teknolojinin gelişmesiyle birlikte

“ Bir hemşire çağrı sistemi yalnızca yardım istemeyi sağlamaz; doğru bilginin doğru kişiye en kısa sürede ulaşmasını sağlayarak sağlık hizmetinin görünmeyen koordinasyon merkezine dönüşür.

hasta beklentileri de değişmektedir. Günümüz hastaları yalnızca kaliteli tedavi değil, aynı zamanda hızlı iletişim, güvenli bakım ve kesintisiz hizmet beklemektedir. Sağlık çalışanları ise yoğun iş temposu içerisinde zamanlarını daha verimli kullanabilecekleri dijital çözümlere ihtiyaç duymaktadır. Hemşire çağrı sistemleri tam da bu iki beklentinin kesişim noktasında yer almaktadır.

Hemşire Çağrı Sistemi Nedir?

Hemşire çağrı sistemi en genel tanımıyla hasta ile sağlık personeli arasında hızlı, güvenilir ve kesintisiz iletişim kurulmasını sağlayan elektronik haberleşme altyapısıdır. Ancak günümüzde bu tanım oldukça yetersiz kalmaktadır. Çünkü yeni nesil sistemler yalnızca hasta çağrılarını ileten cihazlar olmaktan çıkmış, sağlık tesislerinin operasyonel yöneti-



minde aktif rol üstlenen dijital platformlara dönüşmüştür. Modern bir hemşire çağrı sistemi, hasta odalarındaki çağrı terminaleri, koridor ikaz panelleri, merkezi yazılım sunucuları, mobil personel uygulamaları, sesli görüşme altyapıları, acil durum yönetim modülleri ve raporlama yazılımlarından oluşan bütünlüklü bir yapıdır. Bu sistemler aynı anda binlerce cihazdan gelen bilgiyi işleyebilmekte ve farklı öncelik seviyelerine göre yönlendirme yapabilmektedir. Örneğin bir hastanın normal yardım talebi ile kalp durması nedeniyle verilen mavi kod alarmı aynı öncelikte değerlendirilmez. Yazılım, acil durum çağrılarını otomatik olarak en üst öncelik seviyesine taşıyarak ilgili ekipleri eş zamanlı biçimde haberdar eder. Aynı şekilde sağlık çalışanının panik butonuna basması halinde alarm yalnızca hemşire bankosuna değil, güvenlik merkezine, ilgili yöneticilere ve mobil güvenlik ekiplerine de ulaştırılabilir. Bu yaklaşım sayesinde iletişim yalnızca tek yönlü olmaktan çıkmakta, hastanenin farklı birimleri arasında çok katmanlı bir koordi-

nasyon ağı oluşmaktadır. Böylece bilgi kaybı, yanlış yönlendirme ve gecikmeler önemli ölçüde azaltılmaktadır.

Analog Sistemlerden Akıllı Hastanelere

Hemşire çağrı sistemlerinin gelişimi sağlık teknolojilerindeki dönüşümün önemli örneklerinden biridir. İlk nesil sistemlerde hasta yatağındaki butona basıldığında yalnızca ilgili odanın lambası yanıyor ve hemşire çağrısı görsel olarak takip ediyordu. Bu yapı küçük hastaneler için yeterli olsa da büyük sağlık kampüslerinde ciddi sınırlamalar ortaya çıkardı. Aynı anda çok sayıda çağrının gelmesi durumunda hangi hastanın daha öncelikli olduğu anlaşılamıyor, çağrıların cevaplanma süreleri ölçülemiyor ve personelin gerçekten müdahale edip etmediği kayıt altına alınamıyordu. Yönetim açısından bakıldığında ise sistemlerin performansını değerlendirecek herhangi bir veri üretilmiyordu. Dijital dönüşümle birlikte geliştirilen IP tabanlı hemşire çağrı sistemleri bu sorunların büyük bölümünü ortadan kaldırdı. Artık her hasta odası hastane ağına

“ Bir çağrının ne kadar sürede karşılandığını ölçemeyen bir hastane, hizmet kalitesini de tam olarak ölçemez. Dijital hemşire çağrı sistemleri bu görünmeyen performansı görünür hale getirir.

bir parçası olarak çalışmakta, tüm çağrılar merkezi yazılımlar üzerinden yönetilmektedir. Çağrının hangi odadan geldiği, hangi personelin görevlendirildiği, müdahalenin kaç dakika sürdüğü ve çağrının nasıl sonuçlandığı ayrıntılı biçimde kayıt altına alınmaktadır.

Bu kayıtlar yalnızca teknik amaçlarla kullanılmamaktadır. Aynı zamanda kalite yönetimi, hasta memnuniyeti, akreditasyon süreçleri ve personel planlaması açısından da önemli veriler sunmaktadır. Böylece hemşire çağrı sistemi pasif bir iletişim aracı olmaktan çıkarak yöneticilerin karar alma süreçlerini destekleyen stratejik bir bilgi sistemi haline gelmektedir.

Hasta Güvenliğinin İlk Halkası

Hasta güvenliği kavramı yalnızca doğru ilacın doğru hastaya verilmesi veya enfeksiyonların önlen-

**ViYA ;
MOBOTIX C71 ile Yapay
Zeka Destekli 7/24 Akıllı
Hasta Bakıcı**

- ✓ **Düşme Algılama** –
Anında tespit, hızlı
müdahale
 - ✓ **Gün Boyu Gerçek
Zamanlı Destek** –
Kesintisiz takip, maksimum
güvenlik
 - ✓ **MOBOTIX HUB ile
Sorunsuz Entegrasyon** –
Mevcut sistemlere
zahmetsiz uyum
- ViYA ile hasta bakımında
yeni bir çağ başlatın!**



ViYA; Yapay Zeka Destekli 7/24 Akıllı Hasta Bakıcı Sistemi

- **360° Kesintisiz Takip** – Her açıdan tam kontrol, eksiksiz hasta gözetimi
- **GDPR Uyumlu Gizlilik** – Güvenli ve etik veri koruma standartları
- **Gelişmiş İzleme Lisansı** – Profesyonel ve yüksek hassasiyetli izleme teknolojisi
- **Kolay Entegrasyon** – Mevcut sistemlerle zahmetsiz uyum
- **Yüksek Güvenlik & Erken Müdahale** – Riskleri önceden tespit eden akıllı analizler
- **Bakım Personeline Destek** – İş yükünü azaltan verimli asistan
- **Maksimum Esneklik** – Farklı bakım ortamlarına kolay uyum
- **Dayanıklılık & Maliyet Verimliliği** – Uzun ömürlü, ekonomik çözüm

ViYA ile geleceğin hasta bakımını bugünden deneyimleyin!

Uluslararası Kabul Edilmiş Sertifikalar



Alev oluşmadan önce
yangınları tesbit edin.

Hocapaşa Mah. Nöbethane Cad.
No:19 Fatih - İstanbul
Tel: +90 532 767 0444
90 532 211 3038
E-mail: info@viyagroup.net
haterettin@viyagroup.net

“ Bir çağrının ne kadar sürede karşılandığını ölçemeyen bir hastane, hizmet kalitesini de tam olarak ölçemez. Dijital hemşire çağrı sistemleri bu görünmeyen performansı görünür hale getirir.

mesiyle sınırlı değildir. Hastanın ihtiyaç duyduğu anda yardım alabilmesi de güvenli bakımın temel koşullarından biridir. Ameliyat sonrası ayağa kalkmaya çalışan bir hasta baş dönmesi yaşayabilir. Yaşlı bir birey banyoda dengesini kaybedebilir. Solunum sıkıntısı yaşayan bir hasta birkaç saniye içerisinde sağlık personeline ulaşmak isteyebilir. Böyle durumlarda hasta ya da refakatçisinin yardım çağrısını hızlı biçimde iletebilmesi hayati önem taşır. Modern hemşire çağrı sistemleri bu ihtiyaca yalnızca bir buton aracılığıyla cevap vermez. Sesli görüşme özelliği sayesinde hemşire hastayla iletişim kurabilir, durumun aciliyetini değerlendirebilir ve gerekli personeli yönlendirebilir. Gerektiğinde doktor, güvenlik görevlisi veya teknik ekip de aynı iletişim zincirine dahil edilebilir. Araştırmalar, hasta çağrılarını hızlı yanıt verilen servislerde

düşme vakalarının azaldığını, hasta memnuniyetinin yükseldiğini ve sağlık personelinin iş yükünün daha dengeli yönetildiğini göstermektedir. Bu nedenle hemşire çağrı sistemleri artık yalnızca konfor sağlayan teknolojiler değil, hasta güvenliği kültürünün ayrılmaz bir parçası olarak kabul edilmektedir.

Hasta Odasında Başlayan Güvenlik Zinciri

Hasta güvenliğinin sağlanmasında ilk temas noktası hasta odasıdır. Hastanın tedavisinin büyük bölümü bu alanda gerçekleşir ve sağlık personeliyle kurduğu iletişimin önemli kısmı da yine burada başlar. Bu nedenle çağrı sistemlerinin başarısı, yalnızca merkezde kullanılan yazılımın gücüne değil, hasta odasında bulunan ekipmanların ergonomisine, erişilebilirliğine ve kullanım kolaylığına da bağlıdır.

Modern hasta odalarında yatağın başucunda yer alan çağrı ünitesi, artık yalnızca bir çağrı düğmesinden ibaret değildir. Gelişmiş terminaller sayesinde hasta sağlık personeliyle sesli görüşme gerçekleştirebilir, oda aydınlatmasını kontrol edebilir, televizyon ve multimedya sistemlerini kullanabilir, bazı uygulamalarda klima veya perde kontrolünü sağlayabilir. Yemek hizmetleri, temizlik talepleri veya refakatçi istekleri de aynı terminal üzerinden ilgili birimlere iletebilmektedir.

Bu durum ilk bakışta hasta konforunu artıran bir özellik gibi görünse de aslında güvenlik açısından da önemli avantajlar sağlamaktadır. Hastanın yatağından kalkmasına gerek

kalmadan ihtiyaçlarını iletebilmesi, özellikle ameliyat sonrası dönemde düşme riskini önemli ölçüde azaltmaktadır. Aynı zamanda sağlık çalışanlarının hangi talebin tıbbi, hangisinin destek hizmetleriyle ilgili olduğunu önceden görebilmesi, iş akışlarının daha verimli yönetilmesini sağlamaktadır.

Hasta odalarında kullanılan çağrı butonları da ergonomik açıdan sürekli geliştirilmektedir. Özellikle yaşlı hastalar, ortopedik operasyon geçiren bireyler veya hareket kabiliyeti sınırlı kişiler düşünülmüş tasarlanan büyük yüzeyli butonlar, düşük kuvvetle çalışacak şekilde üretilmektedir. Gece kullanımını kolaylaştırmak amacıyla aydınlatmalı tasarımlar tercih edilmekte, kablolu veya kablosuz seçenekler farklı hasta gruplarının ihtiyaçlarına göre belirlenmektedir.

Koridorlarda bulunan kapı üstü ikaz lambaları ise çağrı sisteminin dışarıdan görünen en önemli parçalarından biridir. Sağlık personeli henüz odaya girmeden içeride aktif bir çağrı olup olmadığını bu göstergeler sayesinde anlayabilir. Günümüzde renk kodlu LED teknolojileri kullanılarak farklı alarm türleri birbirinden kolayca ayırt edilebilmektedir. Normal hasta çağrısı, doktor çağrısı, acil çağrı, personelin odada bulunduğunu gösteren durum bilgisi veya teknik arıza uyarıları farklı renklerle ifade edilerek personelin olayın niteliğini daha odaya ulaşmadan değerlendirmesi sağlanmaktadır.

Bu yaklaşım özellikle büyük servislerde gereksiz zaman



kaybını önlemekte ve müdahale sürelerini kısaltmaktadır.

Banyo ve Tuvaletler: Hastanelerin En Riskli Alanlarından Biri

Hasta güvenliği denildiğinde akla çoğunlukla ameliyathaneler, yoğun bakım üniteleri veya acil servisler gelir. Oysa istatistikler hastanelerde meydana gelen düşme vakalarının önemli bölümünün banyo ve tuvaletlerde yaşandığını göstermektedir. Islak zeminler, ani tansiyon düşmeleri, ameliyat sonrası denge kayıpları, yaşlılığa bağlı kas zayıflığı ve kronik hastalıklar bu alanları yüksek riskli bölgeler haline getirmektedir. Bu nedenle çağdaş hemşire çağrı sistemlerinde banyo ve tuvaletler bağımsız güvenlik noktaları olarak ele alınmaktadır. Bu alanlarda kullanılan acil çağrı sistemleri, hastanın yere düşmüş olsa bile yardım isteyebilmesine olanak tanıyacak şekilde tasarlanır. Tavandan

zemine kadar uzanan çekme ipleri veya geniş yüzeyli acil durum butonları sayesinde alarm kolayca oluşturulabilir. Alarmin oluşturulmasının ardından sistem yalnızca hemşire bankosuna bir uyarı göndermekle kalmaz. Olayın gerçekleştiği oda bilgisi merkezi yazılıma aktarılır, koridor ekranlarında ilgili uyarılar görüntülenir, mobil cihaz kullanan sağlık personeline bildirim gönderilir ve gerektiğinde güvenlik merkezi de eş zamanlı olarak bilgilendirilir. Burada dikkat edilmesi gereken önemli noktalardan biri, alarmin yalnızca olay yerine gelen sağlık personeli tarafından iptal edilebilmesidir. Böylece hastanın yanlışlıkla alarmı kapatması engellenirken, gerçekten müdahale edilip edilmediği de kayıt altına alınmaktadır. Bu kayıtlar daha sonra kalite değerlendirmelerinde ve olası hukuki süreçlerde önemli delil niteliği taşıyabilmektedir.

Düşmeyi Önleyen Akıllı Sistemler

Hasta güvenliği yalnızca yardım çağrısına hızlı cevap vermekten ibaret değildir. Asıl hedef, risk oluşmadan önce gerekli önlemleri alabilmektir. Bu nedenle yeni nesil hemşire çağrı sistemleri giderek daha fazla önleyici güvenlik teknolojisiyle entegre çalışmaktadır.

Yatak terk sensörleri bu çözümlerin en yaygın örneklerinden biridir. Özellikle demans hastaları, Alzheimer hastaları, yoğun bakım hastaları veya ameliyat sonrası bilinç bulanıklığı yaşayan bireyler açısından yatağın izinsiz terk edilmesi ciddi risk oluşturabilir. Basınç sensörleri veya akıllı yatak teknolojileri sayesinde hastanın yataktan kalktığı an sistem bunu algılar ve ilgili sağlık personeline otomatik bildirim gönderir.

Son yıllarda görüntü işleme teknolojilerindeki gelişmeler sayesinde yapay zekâ destekli kamera sistemleri de bu alanda kullanılmaya başlanmıştır. Geleneksel hareket algılama sistemlerinin aksine bu kameralar yalnızca hareketi değil, hareketin anlamını da değerlendirebilmektedir. Hastanın gerçekten ayağa kalkmaya çalışıp çalışmadığını, düşme riski oluşturabilecek davranışlar sergileyip sergilemediğini analiz ederek yanlış alarm oranlarını önemli ölçüde azaltmaktadır. Bu tür çözümler özellikle yaşlı bakım merkezlerinde ve rehabilitasyon kliniklerinde sağlık personelinin sürekli fiziksel gözetim yapma ihtiyacını azaltırken, hasta güvenliğini de

önemli ölçüde artırmaktadır.

Personel Güvenliği de Hasta Güvenliği Kadar Önemlidir

Sağlık sektöründe uzun yıllar boyunca güvenlik kavramı büyük ölçüde hastaların korunması üzerine şekillenmiştir. Ancak son yıllarda sağlık çalışanlarına yönelik fiziksel ve sözlü şiddet olaylarının artması, bu bakış açısının değişmesine neden olmuştur. Güvende olmayan bir sağlık çalışanının kaliteli sağlık hizmeti sunması mümkün değildir.

Bu nedenle modern hemşire çağrı sistemleri artık yalnızca hastaların değil, sağlık personelinin de güvenliğini sağlayan çözümler olarak geliştirilmektedir. Özellikle acil servisler, psikiyatri klinikleri, yoğun bakım üniteleri ve gece nöbetlerinin yoğun olduğu bölümlerde çalışan personel için geliştirilen panik alarm sistemleri bunun en önemli örneklerinden biridir. Günümüzde birçok sağlık kuruluşunda hemşireler ve doktorlar görünümü normal bir kimlik kartından farksız olan akıllı personel kartları taşımaktadır. Bu kartların üzerinde bulunan gizli alarm düğmesine basıldığında sistem olayın gerçekleştiği konumu anında belirleyerek güvenlik merkezine iletebilmektedir. Aynı teknoloji bileklik, akıllı saat veya taşınabilir alarm cihazları üzerinde de kullanılmaktadır.

Alarm oluşturulduğunda güvenlik görevlileri yalnızca yardım çağrısını görmekle kalmaz; olayın hangi odada gerçekleştiğini,



alarmı hangi personelin verdiğini ve olayın zamanını da eş zamanlı olarak öğrenebilir. Gelişmiş sistemlerde alarmın bulunduğu bölgedeki güvenlik kameraları otomatik olarak güvenlik merkezinin ekranına düşmekte ve olay anı canlı olarak izlenebilmektedir. Bu sayede güvenlik ekipleri doğru ekipmanla ve doğru sayıda personelle olay yerine yönlendirilebilmektedir.

Bu sistemler yalnızca fiziksel müdahaleyi hızlandırmakla kalmamakta, aynı zamanda sağlık çalışanlarının kendilerini daha güvende hissetmelerini sağlayarak çalışma motivasyonunu da olumlu yönde etkilemektedir.

Acil Durum Yönetiminde Hemşire Çağrı Sistemlerinin Rolü

Sağlık kuruluşlarında her çağrı aynı öneme sahip değildir. Bazı çağrılar hastanın günlük ihtiyaçlarını karşılamaya yönelik rutin taleplerden oluşurken, bazıları ise saniyeler içerisinde müdahale edilmediği takdirde yaşamı tehdit eden sonuçlar

doğurabilecek kritik olaylardır. Bu nedenle modern hemşire çağrı sistemleri yalnızca çağrıyı ileten değil, çağrıları öncelik sırasına koyarak yöneten akıllı platformlar olarak tasarlanmaktadır.

Hastanelerde uygulanan acil durum kodları bu yönetim anlayışının temelini oluşturur. Türkiye’de sağlık kuruluşlarında en yaygın kullanılan kodlar arasında Mavi Kod, Beyaz Kod, Kırmızı Kod, Pembe Kod ve Turuncu Kod yer almaktadır. Her kod farklı bir olay türünü ifade eder ve ilgili ekiplerin en kısa sürede doğru noktaya ulaşmasını amaçlar.

Geçmişte bu kodlar çoğunlukla telefon santralleri veya dahili anons sistemleri üzerinden yürütülüyordu. Ancak büyük kampüs hastanelerinde binlerce kişinin aynı anda bulunduğu düşünüldüğünde, yalnızca sesli anons sistemlerine güvenmek hem zaman kaybına hem de iletişim hatalarına neden olabilmektedir.

Yeni nesil hemşire çağrı sis-

“Bazı sistemlerde çağrının ardından geçen süre saniye hassasiyetinde kayıt altına alınmakta, ekibin olay yerine ulaşma zamanı ve müdahalenin başlangıç süresi raporlanmaktadır.

temleri ise bu süreci tamamen dijital hale getirmektedir. Alarm oluşturulduğu anda sistem olayın türünü analiz ederek önceden tanımlanmış senaryoları otomatik olarak devreye alır. İlgili ekiplere mobil bildirim gönderilir, güvenlik merkezi bilgilendirilir, gerektiğinde koridor ekranları uyarı moduna geçer ve olayın gerçekleştiği bölgedeki kamera görüntüleri otomatik olarak izleme merkezine aktarılır.

Bu otomasyon sayesinde hem bilgi kaybı önlenmekte hem de insan kaynaklı gecikmeler önemli ölçüde azaltılmaktadır.

Mavi Kod: Zamana Karşı Yarış

Mavi Kod uygulaması, kalp veya solunum durması gibi yaşamı doğrudan tehdit eden olaylarda kullanılan en kritik acil durum prosedürlerinden biridir. Böyle bir durumda ilk birkaç dakika içerisinde gerçekleştirilecek

doğru müdahale, hastanın yaşam şansını belirleyen en önemli faktörlerden biridir. Hemşire çağrı sistemleri Mavi Kod sürecinde yalnızca alarm iletmekle kalmaz; aynı zamanda müdahale organizasyonunun koordinasyonunu da üstlenir. Alarmın oluşturulmasıyla birlikte olayın gerçekleştiği konum, ilgili ekibin mobil cihazlarına ve merkezi izleme yazılımına eş zamanlı olarak iletilir. Büyük hastanelerde farklı katlarda görev yapan ekipler arasında en yakın personelin otomatik olarak belirlenmesi, müdahale süresini önemli ölçüde kısaltmaktadır.

Bazı sistemlerde çağrının ardından geçen süre saniye hassasiyetinde kayıt altına alınmakta, ekibin olay yerine ulaşma zamanı ve müdahalenin başlangıç süresi raporlanmaktadır. Bu veriler hem kalite yönetimi hem de eğitim süreçleri açısından önemli performans göstergeleri oluşturmaktadır.

Beyaz Kod ve Sağlık Çalışanlarının Güvenliği

Son yıllarda sağlık çalışanlarına yönelik şiddet olaylarının artması, hastanelerde güvenlik teknolojilerinin önemini daha da artırmıştır. Sağlık çalışanlarının güvenliği artık yalnızca güvenlik görevlilerinin sorumluluğu olarak görülmemekte; teknolojik altyapılarla desteklenen bütüncül bir güvenlik yaklaşımı benimsenmektedir.

Bu noktada hemşire çağrı sistemleri önemli bir görev üstlenmektedir. Sağlık personelinin üzerinde taşıdığı panik

butonları veya mobil uygulamalar aracılığıyla oluşturulan Beyaz Kod alarmı, güvenlik ekiplerine olayın gerçekleştiği konumu anında bildirebilmektedir. IP tabanlı sistemlerde alarm yalnızca bir bildirim olarak kalmaz. Kamera yönetim sistemiyle entegrasyon sayesinde olayın yaşandığı alanın görüntüleri otomatik olarak güvenlik merkezinde açılır. Erişim kontrol sistemleriyle entegre çalışan yapılarda güvenlik görevlilerinin geçiş öncelikleri değiştirilebilir, belirli kapılar otomatik olarak açılabilir ve olay yerine ulaşım hızlandırılabilir.

Bu entegrasyonlar, güvenlik teknolojilerinin birbirinden bağımsız çalışan sistemler olmaktan çıkarak ortak bir güvenlik ekosistemi oluşturduğunu göstermektedir.

Mobil Teknolojiler Sağlık Hizmetlerini Dönüştürüyor

Sağlık sektöründe mobil teknolojilerin kullanımının artması hemşire çağrı sistemlerini de önemli ölçüde değiştirmiştir. Günümüzde sağlık personelinin sabit hemşire bankalarına bağımlı kalmasına gerek yoktur. Akıllı telefonlar, tabletler, DECT telefonlar ve giyilebilir cihazlar sayesinde tüm çağrılar anlık olarak ilgili personele ulaştırılabilmektedir.

Bu durum özellikle büyük kampüs hastanelerinde önemli avantaj sağlamaktadır. Sağlık çalışanı başka bir odada işlem yaparken bile yeni gelen çağrıyı görebilmekte, çağrının içeriğini değerlendirebilmekte ve gerekirse başka bir ekip arkadaşına



yönlendirebilmektedir.

Mobil uygulamalar aynı zamanda çağrının kabul edilmesi, yönlendirilmesi ve sonuçlandırılması süreçlerini de kayıt altına almaktadır. Böylece hangi çağrının kim tarafından karşılandığı, müdahalenin ne kadar sürdüğü ve çağrının nasıl sonuçlandığı ayrıntılı biçimde raporlanabilmektedir.

Bu yaklaşım yalnızca personelin verimliliğini artırmakla kalmamakta, hastaların bekleme sürelerini de önemli ölçüde azaltmaktadır.

Verinin Gücü: Hemşire Çağrı Sistemleri Bir Yönetim Aracına Dönüşüyor

Dijitalleşmenin en büyük avantajlarından biri ölçülebilirliktir. Modern hemşire çağrı sistemleri her gün binlerce

veri üretmektedir. İlk bakışta yalnızca teknik kayıtlar gibi görünen bu bilgiler, doğru analiz edildiğinde hastane yönetimine son derece değerli içgörüler sunmaktadır.

Örneğin belirli bir serviste gece saatlerinde çağrı yoğunluğunun arttığı görülebilir. Başka bir bölümde ise çağrı cevaplama sürelerinin diğer servislere göre daha uzun olduğu tespit edilebilir. Yaşlı hastaların bulunduğu odalarda yardım taleplerinin daha sık geldiği veya belirli saatlerde personel ihtiyacının arttığı kolaylıkla analiz edilebilir.

Bu veriler yöneticilerin personel planlamasını bilimsel verilere dayandırmasını sağlar. Aynı zamanda kalite yönetim sistemleri, akreditasyon süreçleri ve hasta memnuniyeti çalışmalarında objektif performans göstergeleri olarak kullanılabilir.

Artık yalnızca çağrının yapılması değil, çağrının ne kadar sürede karşılandığı, müdahalenin etkinliği ve hasta memnuniyetine etkisi de ölçülebilmektedir.

Siber Güvenlik: Yeni Nesil Risk Alanı

Hemşire çağrı sistemlerinin IP tabanlı yapılara dönüşmesi beraberinde yeni güvenlik sorumlulukları da getirmiştir. Günümüzde bu sistemler hastanenin bilgi ağı üzerinde çalıştığı için siber saldırılara karşı korunmaları büyük önem taşımaktadır.

Bir çağrı sisteminin çalışamaz hale gelmesi yalnızca teknik bir

arıza olarak değerlendirilemez. Böyle bir durumda hasta güvenliği doğrudan etkilenebilir, acil durum çağrıları gecikebilir ve sağlık hizmetinin sürekliliği zarar görebilir.

Bu nedenle üreticiler artık sistemlerini yalnızca donanım güvenliği açısından değil, siber güvenlik açısından da geliştirmektedir. Şifreli veri iletişimi, çok faktörlü kimlik doğrulama, ağ segmentasyonu, düzenli yazılım güncellemeleri ve olay kayıtlarının sürekli izlenmesi günümüz sistemlerinin standart bileşenleri arasında yer almaktadır.

Ayrıca kritik sağlık tesislerinde yedek sunucu mimarileri, kesintisiz güç kaynakları ve felaket kurtarma senaryoları sayesinde olası sistem kesintilerinin hasta bakımını etkilememesi hedeflenmektedir.

Yapay Zekâ ve Akıllı Hastanelerin Geleceği

Önümüzdeki yıllarda hemşire çağrı sistemleri yalnızca yardım çağrılarının yönetildiği platformlar olmaktan çıkarak karar destek sistemlerinin önemli bir parçası haline gelecektir. Yapay zekâ destekli algoritmalar sayesinde hastaların davranış modelleri analiz edilebilecek, düşme riski önceden tahmin edilebilecek ve sağlık personelinin iş yükü dinamik olarak planlanabilecektir.

Giyilebilir sağlık teknolojilerinden elde edilen biyometrik veriler, oda sensörlerinden gelen hareket bilgileri ve elektronik hasta kayıtları tek bir plat-

“ Mobil uygulamalar aynı zamanda çağrının kabul edilmesi, yönlendirilmesi ve sonuçlandırılması süreçlerini de kayıt altına almaktadır. Böylece hangi çağrının kim tarafından karşılandığı, müdahalenin ne kadar sürdüğü ve çağrının nasıl sonuçlandığı ayrıntılı biçimde raporlanabilmektedir.

formda değerlendirilerek olası riskler daha oluşmadan sağlık çalışanlarına bildirilebilecektir. Bu yaklaşım, reaktif güvenlik anlayışından proaktif güvenlik anlayışına geçişin en önemli göstergelerinden biridir. Önümüzdeki dönemde sesle çalışan çağrı sistemleri, yapay zekâ destekli sanal sağlık asistanları, dijital ikiz teknolojileri ve Nesnelerin İnterneti tabanlı hasta odaları sağlık tesislerinin standart bileşenleri haline gelecektir. Böylece hemşire çağrı sistemleri yalnızca bir haberleşme altyapısı değil, hastanenin dijital zekâ merkezlerinden biri olarak konumlanacaktır. Sağlık hizmetlerinde güvenlik kavramı artık yalnızca fiziksel önlemlerle açıklanabilecek kadar dar bir çerçeveye sahip değildir. Günümüz hastanelerinde güvenlik; doğru bilginin doğru kişiye doğru zamanda ulaştırılması, hasta ve sağlık çalışanlarının risklere karşı korunması, acil durumların etkin biçimde yönetilmesi ve tüm süreçlerin kesintisiz olarak sürdürülebilmesi anlamına

gelmektedir. Bu bütüncül yaklaşımın merkezinde ise hemşire çağrı sistemleri yer almaktadır. Modern hemşire çağrı sistemleri, hasta ile sağlık çalışanı arasındaki iletişimi sağlayan basit teknolojiler olmaktan çok daha fazlasını ifade etmektedir. Hastane bilgi yönetim sistemlerinden güvenlik kameralarına, erişim kontrol çözümlerinden bina otomasyonuna kadar pek

çok farklı altyapıyla entegre çalışan bu sistemler, sağlık tesislerinin dijital iletişim omurgasını oluşturmaktadır. Aynı zamanda ürettikleri veriler sayesinde yöneticilere süreçleri analiz etme, kaynakları daha verimli kullanma ve hizmet kalitesini sürekli iyileştirme olanağı sunmaktadır. Akıllı hastanelerin yaygınlaştığı, yapay zekâ ve büyük veri teknolojilerinin sağlık hizmetlerini yeniden şekillendirdiği günümüzde hemşire çağrı sistemleri de bu dönüşümün en stratejik bileşenlerinden biri olmaya devam edecektir. Çünkü hastane ne kadar büyük, teknoloji ne kadar gelişmiş olursa olsun, ihtiyaç duyulan anda doğru yardımın gecikmeden ulaşmasını sağlayan sistemler, sağlık hizmetlerinin görünmeyen ama vazgeçilmez kahramanları olmayı sürdürecektir.



Sağlık Hizmetlerinde Yapay Zekâ Destekli Akıllı Sensör Teknolojisi

Yapay zekâ destekli video analiz teknolojileri, hastaneler, yaşlı bakım merkezleri, rehabilitasyon kuruluşları ve bakım evlerinde güvenlik anlayışını yeniden tanımlıyor.

O. Oryal ÜNVER / ÖGF (Özel Güvenlik Federasyonu) Yönetim Kurulu Başkanı



Hasta Güvenliğinde Yeni Nesil Yaklaşım

Yapay zekâ destekli video analiz teknolojileri, hastaneler, yaşlı bakım merkezleri, rehabilitasyon kuruluşları ve bakım evlerinde güvenlik anlayışını yeniden tanımlıyor. MOBOTIX NurseAssist, yalnızca olayları izleyen bir sistem değil; olası riskleri önceden algılayan, bakım ekiplerini anında bilgilendiren ve hasta güvenliğini proaktif olarak destekleyen akıllı bir çözümdür.

MOBOTIX'un gelişmiş video sensörleri; hareketleri, davranışları ve çevresel değişimleri gerçek zamanlı analiz ederek sağlık personeline anlık ve doğru bilgiler sunar. Böylece güvenlik süreçleri otomatikleşirken bakım kalitesi de önemli ölçüde yükselir.

MOBOTIX NurseAssist'in Sağladığı Avantajlar

Hasta ve Sakin Güvenliğini Artırır
Yapay zekâ destekli analiz sayesinde düşme, yataktan kalkma, uzun süre hareketsiz kalma veya

riskli davranışlar anında tespit edilir. Sistem, bakım personeline gecikmeden uyarı göndererek hızlı müdahale imkânı sağlar.

Personel Verimliliğini Yükseltir

Sürekli fiziksel gözlem ihtiyacını azaltarak sağlık çalışanlarının zamanını daha verimli kullanmasına yardımcı olur. Personel, rutin kontroller yerine doğrudan hasta bakımına odaklanabilir.

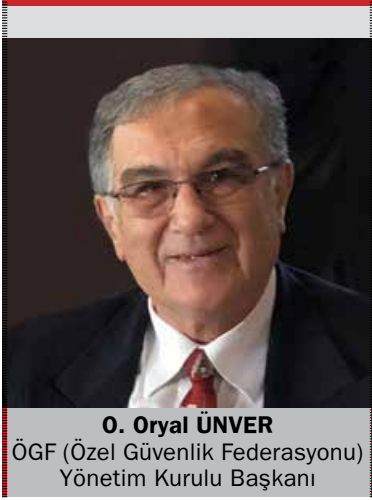
Operasyonel Verimlilik Sağlar

Olayların azalması, daha etkin iş gücü yönetimi ve hızlı müdahale sayesinde kurumların operasyonel maliyetleri düşerken yatırımın geri dönüşü (ROI) önemli ölçüde artar.

Kişiselleştirilmiş ve Önleyici Bakım

Her bireyin hareket alışkanlıkları farklıdır. MOBOTIX NurseAssist, uzun süreli davranış analizleri gerçekleştirilerek kişiye özel risk profilleri oluşturur.

Örneğin; uzun süre yatağın kenarında oturan bir hasta olağan dışı gece hareketleri, hareket sıklığın-



O. Oryal ÜNVER
ÖGF (Özel Güvenlik Federasyonu)
Yönetim Kurulu Başkanı

da ani değişiklikler, düşme riski oluşturan davranış örüntüleri, erken aşamada tespit edilerek bakım ekiplerine bildirilir. Böylece olası kazalar gerçekleşmeden önce önleyici müdahale yapılabilir.

Mevcut Sistemlerle Tam Entegrasyon

MOBOTIX NurseAssist;

- ▮ Hemşire çağrı sistemleri
- ▮ Hastane otomasyonları
- ▮ Acil durum yönetim sistemleri
- ▮ Güvenlik yazılımları
- ▮ Üçüncü taraf uygulamalar ile kolayca entegre olarak sağlık tesislerinde bütünsel bir güvenlik ekosistemi oluşturur.

Yaşlı Bakım Merkezleri İçin Akıllı Güvenlik

Yaşlı bakım merkezlerinde düşmeler, amaçsız dolaşma ve sağlık riskleri en önemli güvenlik sorunları arasında yer alır.

MOBOTIX NurseAssist;

- ▮ Düşme algılama
- ▮ Yatak terk uyarıları
- ▮ Davranış analizi
- ▮ Gece güvenlik kontrolü
- ▮ Gerçek zamanlı alarm yönetimi

özellikleriyle bakım personeline 7/24 destek sağlayarak daha güvenli yaşam alanları oluşturur.

Evde Bakım Çözümleri

Bağımsız yaşayan bireylerin güvenliğini artırmak amacıyla geliştirilen sistem;

- ▮ Acil durumların anında tespit edilmesini,
- ▮ Günlük yaşam rutinlerinin izlenmesini,
- ▮ Olası sağlık problemlerinin erken fark edilmesini,
- ▮ Yakınların ve bakım ekiplerinin hızlı şekilde bilgilendirilmesini sağlayarak evde bakım hizmetlerine yeni bir güvenlik standardı kazandırır.

Engelli Bakım ve Rehabilitasyon Merkezleri

Engelli bireylerin güvenliğini desteklemek amacıyla geliştirilen çözüm;

- ▮ Yatak çıkışlarının algılanması
- ▮ Düşme tespiti
- ▮ Hareket takibi
- ▮ Acil durum bildirimleri sayesinde bakım personelinin hızlı ve doğru karar almasına yardımcı olur.

Veri Güvenliği Önceliğimizdir

Sağlık sektöründe güvenlik yalnızca fiziksel koruma ile sınırlı değildir. Hasta verilerinin korunması da en az hasta güvenliği kadar önemlidir.

MOBOTIX sensörleri;

- ▮ Uçtan uca veri şifreleme
 - ▮ Güvenli uzaktan erişim
 - ▮ Parola koruması
 - ▮ Cactus Concept siber güvenlik mimarisi ile maksimum veri güvenliği sağlar.
- Ayrıca sistem, GDPR ve HIPAA standartlarına uygun gizlilik yaklaşımıyla geliştirilmiş olup etik yapay zekâ prensiplerini esas almaktadır.

Hızlı Kurulum, Kolay Entegrasyon

MOBOTIX NurseAssist, mevcut altyapıya kolayca entegre olacak şekilde tasarlanmıştır. Uzman entegrasyon ekibi sayesinde kurulum süreci günlük operasyonları kesintiye uğratmadan tamamlanır. Kısa devreye alma süresi, güçlü teknik destek ve kullanıcı dostu yapı sayesinde tesisiniz, yapay zekâ destekli güvenlik teknolojisinin avantajlarından çok kısa sürede yararlanmaya başlayabilir.



Fabrikalarda Yapay Zekanın Başarısı

Veri Mimarisinden Geçiyor

WIN EURASIA 2026'da sektör paydaşlarıyla buluşan kurumsal yazılım pazarının küresel oyuncularından Industrial Application Software (IAS), Canias'ın ERP, IoT, büyük veri ve karar destek kabiliyetleriyle üretim sahalarından gelen veriyi süreç bağlamına taşıyan bütünleşik dijital dönüşüm yaklaşımını paylaştı. IAS, üretimde yapay zekanın değer yaratabilmesi için güvenilir veri mimarisi, gerçek zamanlı görünürlük ve entegre süreç yönetiminin kritik hale geldiğini vurguluyor.

CANDOĞAN OLGUN / IAS YAPAY ZEKA İŞ GELİŞTİRME DİREKTÖRÜ

Üretim şirketleri için dijital dönüşüm gündemi; otomasyon, nesnelerin interneti (IoT), veri analitiği ve yapay zeka destekli karar alma süreçleri etrafında yeniden şekilleniyor. Deloitte'un 2026 Manufacturing Industry Outlook raporuna göre, üretim yöneticilerinin yüzde 80'i operasyonel gelişim için ayırdıkları kaynağın en az yüzde 20'sini akıllı üretim projelerine yönlendirmeyi planlıyor. Raporda bu yatırımların otomasyon donanımı, veri analitiği, sensörler ve bulut bilişim gibi temel teknolojilere odaklandığı; üreticilerin akıllı üretimi önümüzdeki üç yılda rekabetçiliğin ana itici güçlerinden biri olarak gördüğü belirtiliyor.



Bu dönüşüm, fabrikalarda rekabet gücünün sahadan gelen verinin hızı, güvenilirliği ve karar süreçleriyle kurduğu bağ üzerinden şekillendiğini gösteriyor. Makine, hat, sensör, enerji tüketimi, duruş, bakım ve kalite süreçlerinden gelen veriler; üretim emri, sipariş, maliyet, stok ve planlama bilgileriyle birlikte ele alındığında şirketler daha güçlü bir karar zemini kazanıyor. Yapay zeka uygulamaları da bu bütünlüklü veri yapısı üzerinde daha sağlıklı analiz, öngörü ve karar desteği üretebiliyor.

Geçtiğimiz günlerde İstanbul Fuar Merkezi'nde düzenlenen 32. Uluslararası Otomasyon ve Makine Teknolojileri Fuarı WIN EURASIA'da sektör paydaşlarıyla buluşan IAS, Canias platformunun ERP, IoT, veri analitiği ve yapay zeka odaklı yaklaşımıyla üretim şirketlerinin sahadan gelen veriyi operasyonel karar gücüne nasıl dönüştürebildiğini paylaştı.

Üretimde yapay zeka için güvenilir veri mimarisi öne çıkıyor

Üretim sahalarında otomasyon seviyesi yükseldikçe makinelerden, hatlardan, sensörlerden ve kalite kontrol noktalarından gelen veri hacmi de artıyor. Bu verinin şirket için değer üretmesi, operasyonel süreçlerle doğru ilişkilendirilebilmesine bağlı. Bir makinenin çalışma süresi, bir hattın duruş verisi, enerji tüketimi ya da kalite sapması; üretim emri, sipariş, malzeme, maliyet ve bakım



CANDOĞAN OLGUN

geçmişleriyle birlikte değerlendirildiğinde karar alma süreçlerine doğrudan katkı sağlayabiliyor. Yapay zeka bu noktada üretim şirketleri için yeni bir karar destek katmanı oluşturuyor. Üretim planlama, kapasite kullanımı, anomali tespiti, kalite kontrol, bakım yönetimi, enerji tüketimi ve sürdürülebilirlik performansı gibi alanlarda yapay zeka uygulamalarının üreteceği değeri; beslediği verinin doğruluğu, sürekliliği ve süreç bağlamı belirliyor. Bu nedenle endüstriyel yapay zeka uygulamalarında güvenilir veri altyapısı, gerçek zamanlı görünürlük ve entegre süreç mimarisi birlikte ele alınması gereken başlıklar arasında yer alıyor.

Canias, sahadaki veriyi süreç bağlamına taşıyor

Canias'ın bütünlüklü yapısı, ERP, IoT, büyük veri ve karar destek kabiliyetlerini aynı dijital omurga üzerinde ele alarak üretim şirketlerinin sahadan gelen veriyi iş süreçleriyle birlikte yönetmesini sağlıyor. Canias

IoT Gateway, ERP sunucuları ile kontrol birimleri, sensörler ve akıllı cihazlar arasında iki yönlü bağlantı kurarak kaynak tüketimi ve çevresel değerler gibi verilerin gerçek zamanlı izlenmesini, analiz edilmesini ve görselleştirilmesini destekliyor. Önceden tanımlanmış kurallar tetiklendiğinde izlenen veriler otomatik olarak ERP çözümüne aktarılabilir.

Canias Üretim Zekası (PRI) modülü, otomasyon ve IoT araçlarıyla toplanan veriler üzerinden gerçek zamanlı raporlama, KPI takibi ve üretim performansının izlenmesi gibi alanlarda şirketlere daha görünür bir operasyon yapısı sunuyor. caniasIQ; veri analizi, çok boyutlu değerlendirme, görselleştirme, özelleştirilebilir gösterge panelleri ve gerçek zamanlı raporlama kabiliyetleriyle karar destek katmanını güçlendiriyor. iasDB'nin farklı veri türlerini destekleyen büyük veri altyapısı ve TROIA'nın esnek geliştirme platformu ise şirketlerin değişen teknoloji ihtiyaçlarına uyum sağlayabilecek güçlü bir dijital zemin oluşturuyor.

Canias'ın bütünlüklü dijital omurga yaklaşımı, yapay zeka uygulamalarının anlamlı ve bağlamlı veriyi çalışmasına zemin hazırlıyor. Üretim sahasından gelen veriler ERP içinde süreç bilgisiyle birleştiğinde; yapay zeka destekli analizler üretim planlamasından kalite yönetimine, bakım süreçlerinden maliyet optimizasyonuna kadar farklı alanlarda daha güçlü karar desteği sunabiliyor. Canias,



bu sayede veriyi izlenen bir unsurdan operasyonel kararların temel girdilerinden birine dönüştürüyor.

IAS Yapay Zeka İş Geliştirme Direktörü Candoğan Olgun, üretimde yapay zekanın değer yaratabilmesi için verinin süreç bağlamıyla birlikte ele alınması gerektiğini belirterek şunları söyledi: “Üretimde yapay zekanın başarısı algoritmanın teknik gücü kadar, verinin hangi süreçten geldiğiyle de bağlantılı. Bir makine verisinin hangi üretim emrine, hangi siparişe,

hangi kalite sonucuna ve hangi maliyet kalemine karşılık geldiğini bilmek, sağlıklı karar desteğinin temel koşulları arasında yer alıyor. IoT sahadan veriyi toplarken, ERP bu veriye iş bağlamı kazandırıyor. Yapay zeka ise bu bütünlük üzerinden üretim şirketlerine öngörü, analiz ve karar desteği sunuyor. WIN EURASIA’da paylaştığımız Canias yaklaşımı da bu entegre yapıya dayanıyor. Canias’ın sunmuş olduğu veri mimarisi ve veri yönetişim (Data Governance)

“Yapay zekanın üretimdeki başarısı veri mimarisiyle doğrudan bağlantılı.

altyapısı, sistemdeki değişken iş alanlarında kullanılan veriler arasındaki bağlamın yapay zeka ile anlamlandırılmasına ve sistemin karar destekleyen ve karar veren bir noktaya erişmesini sağlıyor.”

Deloitte’un 2026 Manufacturing Industry Outlook raporu, ajan tabanlı yapay zeka (agentic AI) uygulamalarının üretimden tedarik zincirine ve ofis süreçlerine kadar farklı alanlarda değer yaratabileceğine dikkat çekerken; ölçekli uygulama için veri, teknoloji, yönetim ve iş akışı dönüşümü gibi başlıkların birlikte değerlendirilmesi gerektiğini ortaya koyuyor. Bu gereklilik, üretim şirketlerinde yapay zeka projeleri için sağlam dijital altyapı, net süreç sahipliği ve güvenilir veri akışının önemini artırıyor.

Fiziksel AI (Physical AI)

Üretim şirketleri için bir diğer önemli gelişme alanı da Fiziksel AI konusu. Toplanan veriler ve iş süreçleri üzerinden karar alan ve karar alma noktasında insanları destekleyen, insan etkileşimi sistemlerin yanında makine etkileşim sistemler de gelişmeye devam ediyor.

IoT altyapısı ile tesislerde kullanılan makineler, otonom sistemler (AGV vb.) ve robotik sistemler ile çift yönlü entegre olarak, şirketin kurumsal hafızası ve iş yapış biçimleri sistemler ile tam entegre ediliyor ve sistemlerin bağımsız çalışması için bir süreç ortaya koyuyor. Bu yapı ile düşünsel seviyedeki kurumsal bilgi fiziksel dünyaya yansıtılmış ve otonom üretim sistemleri oluşturulmuş oluyor. Canias'ın IoT teknolojisi yanına konumlandırılan yapay zeka katmanı ile tam otomatik akıllı fabrikalar gerçeğe dönüşüyor. Darboğazlar tespit edilip üretim ve bakım planlarına göre makineler yönlendiriliyor, kamera gibi algılayıcılar ile kalite sorunları tespit edilebiliyor, anormali tespiti gibi çözümler ile üretim planları ve bakım planları sistemsel ve fiziksel dünyada yönetilebiliyor, AGV ve otomatik konveyör sistemleri ile lojistik süreçler yönetiliyor. Enerji tüketimindeki değişimler, üretim akışları ile ilişkilendirilerek yönetiliyor. Canias'ın IoT ve MES ürünleri ile birlikte çalışan Fiziksel AI katmanı tesislerin dijital dönüşümünü destekliyor.

Yapay zeka üretimde öngörü ve karar desteği katmanı oluşturuyor

Üretim şirketleri için yapay zeka, sahadan gelen verinin daha hızlı anlamlandırılmasını ve operasyonel kararların daha güçlü bir veri temeline oturmasını sağlıyor. Üretim planlarının kapasite verisiyle birlikte de-

ğerlendirilmesi, kalite sapmalarının erken fark edilmesi, bakım ihtiyaçlarının daha öngörülü biçimde ele alınması, enerji tüketimindeki anormalliklerin izlenmesi ve maliyet etkilerinin daha hızlı analiz edilmesi bu dönüşümün öne çıkan kullanım alanları arasında yer alıyor. Canias'ın ERP ve IoT mimarisiyle bütünleşen yapay zeka yaklaşımı, üretim şirketlerinin veri kaynaklarını tek bir operasyonel çerçevede değerlendirmesine destek oluyor. Bu sayede şirketler, sahadan gelen teknik verileri üretim, kalite, maliyet, bakım, sürdürülebilirlik ve raporlama süreçleriyle ilişkili biçimde yönetebiliyor. Böylece yapay zeka, üretim şirketleri için operasyonel görünürlüğü artıran, karar alma süreçlerini hızlandıran ve veriye dayalı yönetim kültürünü güçlendiren bir katmana dönüşüyor. Yapay zekanın üretim şirketleri için sunduğu potansiyelin doğru veri zeminiyle güçlenebileceğini vurgulayan Candoğan Olgun, sözlerini şöyle sürdürdü: "Yapay zeka, üretim şirketleri için sahadaki veriyi daha hızlı anlamlandırma ve operasyonel kararları daha güçlü bir veri temeline oturtma imkanı sunuyor. Bu potansiyelin hayata geçmesi için verinin üretim, bakım, kalite, maliyet ve planlama süreçleriyle birlikte okunması gerekiyor. Bizim yaklaşımımızda yapay zeka, ERP ve IoT mimarisinin doğal devamı olarak konumlanıyor. Canias ile şirketlerin üretim süreçlerinde daha öngörülü, izlenebilir ve



veriye dayalı kararlar almasını sağlıyoruz. Artık ERP sistemleri karar vermek için rapor üreten yapılardan çıkıp şirketler için karar alan veya karar alma noktasında tavsiyeler veren yapılara evriliyor." Endüstriyel dönüşümün yeni aşamasında rekabet gücü; üretim sahasından gelen verinin güvenilir, izlenebilir ve karar süreçlerine entegre biçimde yönetilebilmesiyle şekilleniyor. IAS, Canias'ın ERP, IoT, büyük veri ve karar destek kabiliyetleriyle üretim şirketlerinin dijital dönüşüm yolculuğunda sahadan gelen veriyi daha görünür, anlamlı ve karar odaklı bir yapıya taşımasına destek oluyor.

Güvenlik teknolojilerinde sürdürülebilirlik **artık satın alma kriteri haline geliyor**



Güvenlik teknolojilerinde sürdürülebilirlik artık satın alma kriteri haline geliyor

AXIS

Kuruluşların teknoloji yatırımlarında öncelikleri değişiyor. Performans, siber güvenlik ve toplam sahip olma maliyetinin (TCO) yanı sıra sürdürülebilirlik kriterleri de satın alma kararlarında giderek daha belirleyici hale geliyor. Özellikle güvenlik teknolojileri sektöründe ürünlerin enerji tüketimi, karbon ayak izi, kullanılan malzemeler ve yaşam döngüsü performansı artık değerlendirme süreçlerinin

önemli bir parçası olarak öne çıkıyor. Ağ video çözümlerinde dünya lideri Axis Communications tarafından yayımlanan 2025 Sürdürülebilirlik Raporu, güvenlik sektöründeki bu dönüşümün hız kazandığını ortaya koyuyor. Şirket, büyümesini sürdürürken çevresel etkisini azaltma, sorumlu iş uygulamalarını güçlendirme ve sürdürülebilirliği tüm değer zincirine yayma hedeflerinde önemli ilerlemeler kaydetti.

Güçlü büyüme, uzun vadeli sürdürülebilirlik yaklaşımıyla destekleniyor

Axis Communications, 2025 yılında 2,1 milyar ABD doları satış hacmine ulaşırken, dünya genelindeki çalışan sayısını 5.273'e çıkardı. Şirket, büyümesini sürdürürken aynı zamanda sürdürülebilirlik yatırımlarını artırmaya ve uzun vadeli çevresel hedeflerine odaklanmaya devam etti.

Axis Başkanı ve CEO'su Ray

Mauritsson, raporda yer alan değerlendirmesinde, küresel ölçekte artan jeopolitik belirsizlikler ve değişen iş ortamında uzun vadeli sorumluluk anlayışının her zamankinden daha önemli hale geldiğini vurguluyor. Şirket, sürdürülebilirliği yalnızca çevresel bir hedef olarak değil, iş stratejisinin temel bir unsuru olarak görüyor.

Satın alma ekiplerinin gündemi değişiyor

Kuruluşlar artık güvenlik çözümlerini değerlendirirken yalnızca teknik özelliklere odaklanmıyor. Enerji verimliliği, kullanılan malzemeler, tedarik zinciri şeffaflığı, ürün ömrü ve geri dönüştürülebilirlik gibi kriterler de karar süreçlerinde giderek daha fazla önem kazanıyor. Bu yaklaşım, güvenlik sektöründe “en düşük satın alma maliyeti” anlayışından “uzun vadeli değer ve sürdürülebilirlik” yaklaşımına geçişi hızlandırıyor. Özellikle Avrupa Birliği’nin sürdürülebilirlik ve tedarik zinciri düzenlemeleri, teknoloji üreticilerinin ve kurumsal satın alma ekiplerinin önceliklerini yeniden şekillendiriyor.

Karbon emisyonlarını azaltmak için iddialı hedefler

Axis, iklim değişikliğiyle mücadele kapsamında bilim temelli hedefler belirledi. Şirket, 2030 yılına kadar Scope 1 ve Scope 2 sera gazı emisyonlarını 2022 baz yılına göre yüzde 42 azaltmayı hedefliyor. Bunun yanında satın alınan ürün ve hizmetler, lojistik süreçleri ve satılan ürünlerin kullanımı kaynaklı Scope 3 emisyonlarını da ürün başına

yüzde 51,6 oranında azaltmayı planlıyor. Şirket ayrıca 2030 yılına kadar üretim ve lojistik merkezlerinde kullanılan enerjinin tamamını fosilsiz kaynaklardan sağlamayı hedefliyor. Rapora göre Scope 3 emisyonları, şirketin toplam sera gazı emisyonlarının yaklaşık yüzde 99’unu oluşturuyor ve bu nedenle değer zinciri genelindeki iş birlikleri sürdürülebilirlik stratejisinin önemli bir parçası olarak görülüyor.

Döngüsel ekonomi ve sürdürülebilir ürün tasarımı öne çıkıyor

Axis’in sürdürülebilirlik yaklaşımının merkezinde ürün yaşam döngüsünü uzatmak ve doğal kaynak kullanımını azaltmak yer alıyor. Şirket, yüksek ürün kalitesi, tamir edilebilirlik ve yazılım güncelleme-leri sayesinde ürünlerin kullanım ömrünü uzatmayı hedefliyor. Ayrıca geri dönüştürülmüş ve biyobazlı malzemelerin kullanımını artırarak döngüsel ekonomi yaklaşımını destekliyor. Bu kapsamda Axis, 2028 yılına kadar Axis tasarımı ürünlerde kullanılan plastiklerin en az yüzde 50’sinin yenilenebilir karbon bazlı malzemelerden oluşmasını hedefliyor. Şirket aynı zamanda PVC, bromlu ve klorlu alev geciktirici maddelerin ürünlerden tamamen kaldırılması yönündeki çalışmalarını sürdürüyor. Rapora göre bugün Axis ürünlerinin neredeyse tamamı PVC içermiyor.

Siber güvenlik ve etik teknoloji yaklaşımı sürdürülebilirliğin ayrılmaz parçası
Raporda sürdürülebilirliğin yal-

nızca çevresel etkilerden ibaret olmadığına da dikkat çekiliyor. Axis, insan hakları, etik teknoloji kullanımı, veri gizliliği ve siber güvenliği sürdürülebilirlik yaklaşımının temel bileşenleri arasında değerlendiriyor. Şirketin bilgi güvenliği yönetim sistemi ISO/IEC 27001:2022 standardı doğrultusunda yönetilirken, 2025 yılı boyunca herhangi bir bilgi güvenliği ihlali raporlanmadı. Axis ayrıca insan hakları durum tespiti çalışmaları kapsamında tedarik zinciri ve satış süreçlerinde risk değerlendirmelerini genişletmeye devam etti.

ESG performansında bağımsız doğrulama

Axis’in sürdürülebilirlik performansı bağımsız kuruluşlar tarafından da değerlendiriliyor. Dünyanın önde gelen sürdürülebilirlik derecelendirme kuruluşlarından EcoVadis tarafından gerçekleştirilen son değerlendirmede Axis, değerlendirilen tüm şirketler arasında 81. persentilde yer alarak ESG performansını daha da geliştirdi. Güvenlik teknolojileri sektöründe başarı artık yalnızca görüntü kalitesi, performans veya bağlantı özellikleriyle ölçülüyor. Kuruluşlar için ürünlerin çevresel etkisi, enerji verimliliği, kullanılan malzemeler, siber güvenlik yaklaşımı ve tedarik zinciri şeffaflığı da yatırım kararlarının önemli unsurları haline geliyor. Axis Communications’ın 2025 Sürdürülebilirlik Raporu, sürdürülebilirliğin güvenlik teknolojilerinde giderek daha güçlü bir satın alma kriteri olarak öne çıktığını ortaya koyuyor.

GÜSOD Başkanı Turgay ŞAHAN:

Özel güvenlik hizmetlerinin meslek olarak kabul görebilmesi için **özlük hakları iyileştirilmeli**

Sektörün en eski ve öncü sivil toplum kuruluşu Güvenlik Servisleri Organizasyon Derneği (GÜSOD) Başkanı Turgay ŞAHAN, özel güvenlik görevlilerinin Özel Güvenlik Haftası'nı kutladı.

GÜSOD

Sektörün en eski ve öncü sivil toplum kuruluşu Güvenlik Servisleri Organizasyon Derneği (GÜSOD) Başkanı Turgay ŞAHAN, özel güvenlik görevlilerinin Özel Güvenlik Haftası'nı kutladı. ŞAHAN yaptığı açıklamada, "Toplumumuzun güvenliği ve huzuru için gece gündüz demeden çalışan tüm özel güvenlik görevlilerimizin Özel Güvenlik Haftası'nı en içten dileklerle kutlarım. Özel güvenlik sektöründe kamuya ilişkiler ekseninde gerekli girişimleri yapmaya, kamu ve özel güvenlik iş birliği konularına destek olmaya devam ediyoruz. Özel güvenlik görevlilerinin çalışma koşullarının iyileştirilmesi ve mesleki yeterliliklerinin artırılması için de çalışmayı sürdürüyoruz. Sektördeki çalışma şartlarının iyileştirilmesi ve özlük hakları konu-



sunda düzenlemeler yapılması daha çok kişinin sektörümüze tercih etmesine neden olurken özel güvenlik hizmetlerinin bir meslek olarak kabul görmesini sağlayacaktır." dedi.

GÜSOD Başkanı Turgay ŞAHAN, zor şartlar altında görevlerini yerine getiren 380 bine yakın çalışanın Özel Güvenlik Günü Haftası'nı kutladı.

"Özel güvenlik görevlileri

emeklerinin karşılığını tam olarak almalı"

GÜSOD Başkanı ŞAHAN, Özel Güvenlik Haftası nedeniyle yaptığı açıklamada özel güvenlik görevlilerinin özlük hakları konusunda iyileştirilmeler yapılması gerektiğine dikkat çekerek, "Kamusal ve özel alanlarda güvenliğin sağlanmasında büyük rol oynayan özel güvenlik görevlilerinin emeğinin karşılığını tam olarak alamaması sektörün gelişmesine de engel



TURGAY ŞAHAN

oluyor. Özel güvenlik görevlisi olarak hizmet verenler asgari ücret seviyesinde ya da bu seviyeye yakın maaş almaları ve özlük hakları gibi nedenlerden dolayı sık sık iş değiştiriyorlar. Dolayısıyla özel güvenlik şirketleri sürekli olarak yeni personel arayışına giriyor ve bu durum da talep çok algısına yol açıyor. Sektördeki çalışma şartlarının iyileştirilmesi ve özlük hakları konusunda düzenlemeler yapılması istihdam sorununa çözüm olacak ve daha çok kişinin sektörümüzü tercih etmesini sağlayacaktır.” dedi.

“Özel güvenlik hizmetleri meslek olarak kabul görmeli”

Özel güvenlik hizmetlerinin meslek olarak algılanmasının sektör açısından büyük önem taşıdığının altını çizen ŞAHAN, “Meslek olarak kabul görmesini istediğimiz özel güvenlik hizmetlerinde sektöre yönelik alan eğitimlerinin artırılması gerekmekte. Derneğimiz, özel güvenlik sektöründe hizmet

veren özel güvenlik görevlilerinin yüksek seviyede eğitim almaları ve sektör standartlarının yükseltilmesi konusunda çalışmalar yapmayı sürdürüyor. Üye şirketlerimiz aracılığıyla teknolojik gelişmelerin özel güvenlik sektörüne entegrasyonunu sağlayacak çalışmalara katkıda bulunmaya da devam ediyoruz, ayrıca genel kolluk ile özel güvenlik arasındaki etkin iş birliği ve koordinasyona da önem vererek gerekli iş birliğini yapıyoruz.” şeklinde sözlerini sürdürdü.

“Kamunun desteği sektör için büyük önem taşıyor”

Turgay ŞAHAN, “Kamunun desteği bizler için çok önemli, bu paralelde kamu ve özel güvenlik iş birliği konularına odaklanmayı sürdürüyor, kamuyla ilişkilerimizi aktif tutarak paydaşlarımızı da tüm süreçte dahil ediyoruz. Kamuyla ilişkiler ekseninde gerekli girişimleri yapmayı, kamu ve özel güvenlik iş birliği konularına destek olmayı ve özel güvenlik görevlilerinin mesleki yeterliliklerinin artırılması için çalışmayı sürdürüyoruz. Bu paralelde özel güvenlik sektörünün tercih edilen bir meslek grubu olması yönünde ciddi adımlar atılabileceğini düşünüyoruz.” açıklamasını yaptı.

“Özel güvenlik görevlilerinin çalışma koşulları iyileştirilmeli”

Özel güvenlik görevlilerine cesaretleri ve her zorluğa

GÜSOD Başkanı Turgay ŞAHAN, zor şartlar altında görevlerini yerine getiren 380 bine yakın çalışanın Özel Güvenlik Günü Haftası’nı kutladı.

rağmen verdikleri emekleri için teşekkür eden GÜSOD Başkanı Turgay ŞAHAN, “Her zaman belirttiğimiz gibi Özel Güvenlik Haftası’nda da özel güvenlik görevlilerinin özlük ve yan hakları konusunda iyileştirilmeler yapılması gerektiğinin altını bir kez daha çizmek isteriz. Kamusal ve özel alanlarda güvenliğin sağlanmasında büyük rol oynayan özel güvenlik görevlilerinin emeğinin karşılığını tam olarak alamaması sektörün gelişmesine de engel oluyor. Özel güvenlik sektöründeki yüksek turnover oranının önüne geçmek için çalışma koşullarının, ücretlerin ve özlük haklarının iyileştirilmesi gerekiyor. Önümüzdeki dönemde de özel güvenlik hizmetlerinin kalitesini artırmak, sektörün gelişimini desteklemek ve çalışanların haklarını korumak amacıyla çalışmalar yapmayı sürdüreceğiz, Avrupa’daki sektörün konumu na paralel aksiyonlar alacak ve projeler geliştireceğiz.” şeklinde sözlerini sürdürdü.

Yangın algılama ve ihbar sistemleri

Yapı alanı, yüksekliği, yapıyı kullanan kişi sayısı gibi parametreler büyüdükçe yapı daha karmaşık hale geleceğinden yangın anında insanların tahliye edilmesinin çok zaman almasının yanı sıra, yangının kontrol altına alınması ve söndürülmesi işlemi de güçleşmektedir.

Erdal YILDIZ/ Satış Müdürü
ENTEGRE SATEK

Günümüz dünyasında, toplu olarak yaşama, çalışma, birlikte olma olgusunun artması ve bu amaçlara hizmet edecek yapıların çoğalması; yangının oluşma riskini, risk çeşitliliğini ve hasar verici etkilerini geçmişten bu yana sürekli olarak arttırmaktadır. Yangından doğabilecek hasar ve can kayıplarını azaltmanın en başta gelen yolu, yangını oluşturacak etkenleri ortadan kaldırmak ve yangına hızlı bir şekilde müdahale edebilecek tedbirleri almaktır. Yangın güvenlik önemlerinin alınması, yangının verdiği zararlardan daha az maliyetlidir. Bu da yangının erken tespiti için gerekli olan yangın algılama ve ihbar sistemleri ve diğer yangından korunma sistemlerinin önemini ortaya çıkartmaktadır. Yangın; yanabilen maddelerin çevresine değişik miktarlarda ısı ve ışık yayarak, kontrol dışı yanmasıdır. Yanmanın başlaması ve sürebilmesi için, yanıcı madde, yakıcı madde ve ateşleme kaynağının bir arada olması gerekmektedir.

(Yangın üçgeni). Bir binayı yamaz olarak inşa edilemeyeceğini göz önünde bulundurursak, o halde yapılacak en akıllıca iş onu güvenli hale getirmektir. Yangınların temel çıkma sebepleri, bilgisizlik, tedbirsizlik, ihmal, dikkatsizlik, kazalar, sıçrama, doğa olayları ve sabotaj olarak sıralanabilir. Yangının, hasar verme kapasitesinin dakikalar, hatta saniyeler içinde artarak ilerlemesi, yangın başlangıcı ve sonrasında tedbir ve müdahale amaçlı kullanılacak yangından korunma, yangın algılama ve ihbar sistemlerinin hızlı reaksiyon gösterecek şekilde kurgulanmasını mecbur kılmaktadır.

Yangından Korunma Sistemleri, yangın çıktığı durumlarda, yangının daha başlangıç aşamasında tespiti, yangının yayılmasının yavaşlatılması, mümkünse yok edilmesi için gerekli aksiyonların alınması, insanların en hızlı şekilde tahliye edilmesini sağlayacak sistemlerdir. Biz yazımızda, yangın algılama ve ihbar sistemlerini ele alacağız.

Yangın algılama ve ihbar sistemleri yapılarda çıkabilecek yangınları en kısa sürede tespit etmek, insanların tahliyesi ve gerekli aksiyonların alınması için haberdar etmek, diğer yardımcı sistemleri yangından korunma, tahliye amaçlı işlemler için tetiklemek ve yangın söndürme birimlerine haber vermek amacıyla kurulan sistemlerdir. İnsan tahliyesinin kolay olduğu binalarda, algılama ve uyarma sistemleri bazı durumlarda yeterli görülebilir. Yapı alanı, yüksekliği, yapıyı kullanan kişi sayısı gibi parametreler büyüdükçe yapı daha karmaşık hale geleceğinden (Hasane, AVM, Endüstriyel Tesisler, İş Merkezi, Üniversite Kampüsleri, Havalimanları, Çok Katlı Konutlar vb.) yangın anında insanların tahliye edilmesinin çok zaman almasının yanı sıra, yangının kontrol altına alınması ve söndürülmesi işlemi de güçleşmektedir. Bundan dolayı, bahsetmiş olduğumuz tarzdaki yapılarda, yangın anında can kayıplarının engellenmesi, insanların tahliyesinin sağlanması, dumanın yönlendirilmesi, yangının otomatik söndürme sistemleriyle

söndürülmesi gibi aksiyonların sistematik ve koordineli şekilde yapılması için, yangın algılama ve ihbar sistemlerinin diğer sistemlerle entegrasyonunun yapılması gerekmektedir.

Örneğin; yangın anında, yapıdaki kilitli olan kapıların serbest bırakılıp insanların güvenli şekilde tahliyesinin sağlanması için, kartlı geçiş sistemleri ile entegrasyonun sağlanması gerekmektedir. Tahliye esnasında egzoz ve taze hava fanlarının otomatik olarak devreye sokulup insanların dumandan etkilenmemesi için, duman tahliye sistemleri ile entegrasyon sağlanmalıdır. Ya da söndürme için kullanılan ön tepkimeli sprinkler (Sulu söndürme) sistemi gibi (Pre-action systems) sistemlerinin devreye sokulması yangının algılanmasıyla birlikte yapılmaktadır. Yine burada yangın algılama sistemi ile sprinkler sistemi arasında entegrasyon sağlanmaktadır. Entegrasyonlar, kuru kontak bazında sağlanabileceği gibi, kabiliyeti olan sistemlerle yazılımsal olarak da (OPC vb. protokoller) yüksek seviyeli şekilde sağlanabilmektedir. Yangın algılama ve ihbar sistemleri, yürürlükteki yangından korunma yönetmeliklerine ve ilgili standartlara uygun olarak tasarlanmaktadır. Ülkemizde yürürlükte olan "Binaların Yangından Korunması Hakkında Yönetmelik" 4.Bölüm – Yangın Algılama ve Uyarı Sistemleri Madde 74 -1 uyarınca: "Yangın algılama sisteminin ve parçalarının TS EN 54'e uygun olarak üretilmesi, tasarlanması, tesis edilmesi ve işletilmesi şarttır."

Dolayısıyla sistemin projelendirilmesi, tasarımı, devreye alınması, test edilmesi, işletilmesi ve bakımlarının yapılması TS EN 54 standartlarına uygun olmak zorundadır.

Yönetmelik, sistemin ve ekipmanların bulunması zorunlu olduğu binaları, ekipmanların nasıl yerleştirileceğini ve bazı temel gereksinimleri tarif eder. Ancak sistemin tasarımı, ekipmanların yerleşim kriterleri, işletme detayları ve bakımın yöntemi ve periyotları konularında TS EN 54-14 standartları referans gösterilmiştir.

Ülkeler, kendi spesifik yangın standartlarını oluşturabileceği gibi, (NFPA 72- ABD, FDMA – Japonya) uluslararası kabul görmüş standartları kendilerine uyarlama yoluna da gidebilir (EN -54 – TS EN 54).

Yangın algılama ve ihbar sistemleri 5 ana ekipman bölümünden oluşmaktadır.

Merkez Ekipmanları: Yangın Algılama Sistemi Paneli, Kullanıcı Grafik Ekranı, Tekrarlayıcılar, Mimik Panel (Dizayna Bağlı olarak)

Birincil ve İkincil Güç Kaynakları: Sistem merkez ve saha ekipmanlarının, normal durumda ya da olası bir güç kesintisinde

çalışmasını sağlayacak olan her türlü güç kaynağı.

Algılama ve Manuel Alarm Başlatma Cihazları: Dedektörler, manuel alarm butonları

Sesli Görsel ve Uyarı Cihazları: Siren, Flaşör, Acil Anons Sistemleri

Arayüz Modülleri: Sistemin, kelebek vanalar, akış anahtarları, yangın pompaları, duman tahliye sistemleri ve kartlı geçiş sistemi kapıları gibi diğer sistem ekipmanlarıyla etkileşimi sağlayacak giriş/çıkış modülleri.

Yangın algılama panelinin, sahadaki ekipmanları tanımlayış biçimine göre iki ayrı teknoloji mevcuttur: Konvansiyonel ve Adresli Sistemler. Konvansiyonel sistemler, ekipmanların panel hattına paralel olarak bağlandığı ve ekipmanların kendine özgü lokasyon bilgisini veremediği sistemlerdir. Yani, her bir hat panelde tek bir adres olarak tanımlanabilmektedir. Aynı hat içerisinde, iki farklı dedektör, panel için aynı eleman olarak kabul edilir. Dolayısıyla Alışve



Tüm güvenlik sektörünü kapsayan www.guvenliktedarik.com; güvenlik sektörüne ürün ve hizmet sunan firmalarla nihai kullanıcının buluştuğu bir online alışveriş ve tanıtım sitesidir. Güvenliğin ihtiyaca uygun şekilde tesis edilmesi adına tüm ilgililerin ürün / hizmet alımı ve satımını hedefleyen www.guvenliktedarik.com; en son teknolojiye uygun ürün ve çözümlerden herkesi haberdar eden online platformdur.



- CCTV ve video kontrol sistemleri,
- Yangın algılama ve ihbar sistemleri,
- Yangın söndürme sistemleri,
- Geçiş kontrol sistemleri,
- Hırsız alarm sistemleri,
- Mobil takip sistemleri,
- Alarm izleme merkezleri,
- Apartman konuşma sistemleri,
- Drone teknolojisi

Siber Saldırganların **Kimlik Bilgilerine Dayalı** Saldırı Teknikleri

Parola tahmini ve yetkili hesapların suistimal edilmesi, 2025'te siber suçluların en başarılı sızma yöntemleri oldu. Bu durum, saldırganların artık güvenlik altyapılarına takılan gürültülü zararlı yazılımlardan uzaklaştığını kanıtıyor. Tehdit aktörleri, tespit edilmemek için meşru erişim haklarını kullanmaya başlayarak stratejik bir eksen kayması gerçekleştiriyor.

KASPERSKY



Kaspersky Security Services'in güncel raporuna göre; parola tahmini ve yetkili hesapların suistimal edilmesi, 2025'te siber suçluların en başarılı sızma yöntemleri oldu. Bu durum, saldırganların artık güvenlik altyapılarına

takılan gürültülü zararlı yazılımlardan uzaklaştığını kanıtıyor. Tehdit aktörleri, tespit edilmemek için meşru erişim haklarını kullanmaya başlayarak stratejik bir eksen kayması gerçekleştiriyor. "Siber Dünyanın Anatomisi" başlıklı kapsamlı küresel

rapor; Managed Detection and Response (MDR), Incident Response (IR), Compromise Assessment ve SOC Consulting birimlerinin 2025 yılı boyunca elde ettiği verilere dayanıyor. Çalışmada en sık karşılaşılan saldırgan teknikleri, araçları ve tespit senaryoları incelenirken,

tespit edilen olayların ayırt edici özelliklerine de ışık tutuyor. Rapora göre, en yoğun şekilde izlenen saldırı tekniklerinin büyük bir kısmı kimlik bilgileri ve kimlik yönetimi süreçleri etrafında şekilleniyor. Çeşitli Saldırı Göstergelerinin (IoA) dönüşüm oranlarını* inceleyen analiz, siber tehditlerde öne çıkan şu taktikleri gözler önüne seriyor:

Parola Tahmini (%34,8): Saldırganların bir hesaba erişim sağlamak için sistematik olarak farklı parolaları denediği bu yöntem, dönüşüm listesinin zirvesinde yer alıyor. Tekniğin ilk sırada yer almasının nedeni hem gerçek saldırılarda hem de yetkili güvenlik testlerinde yoğun olarak kullanılması ve günümüz siber güvenlik dünyasında kalıcı bir tehdit oluşturmalarıdır. Zayıf veya yinelenen parolalar kullanan organizasyonlar, bu köklü stratejinin işe yaramasına zemin hazırlamaya devam ediyor.

Yerel Hesap Oluşturma (%34,7): Saldırganlar sisteme bir kez sızdıktan sonra, ilk elde ettikleri erişim noktası fark edilip kapatılsa bile içeride kalmayı sürdürmek için sık sık yeni yerel hesaplar açıyor. Güvenlik tatbikatlarında da sıklıkla gözlemlenen bu teknik, doğru telemetri altyapısıyla tespit edilebiliyor; ancak şirketler genellikle bu görünürlüğü sağlayacak telemetri altyapısı bulunmuyor.

Yetkili Hesapların Suistimal Edilmesi (%34,5): Saldırganlar

sisteme zararlı yazılım bulaştırmak yerine, ele geçirdikleri geçerli kimlik bilgileriyle giriş yaparak normal kullanıcı faaliyetlerinin arasında kamufle oluyor. Erişim süreci tamamen yasal görüldüğü için bu durum tespiti ciddi şekilde zorlaştırıyor. Yüksek dönüşüm oranı, sızdırılan kimlik bilgilerinin neden hâlâ en tehlikeli saldırı vektörlerinden biri olduğunu açıkça kanıtıyor.

Hesap Manipülasyonu (%32): Saldırganlar, içerideki erişimlerini kalıcı kılmak ve pekiştirmek için mevcut hesaplar üzerinde değişiklik yapıyor; devre dışı bırakılmış hesapları yeniden aktif hale getiriyor, grup üyeliklerini değiştiriyor veya yetki yükseltiyor. Bu durum, siber korsanların sisteme yeni araçlar sokmak yerine, halihazırda var olan unsurları kullanarak hakimiyetlerini artırdıklarına dair genel eğilimi destekliyor.

Ağ Servislerinin Keşfi (%31,2): Saldırganlar bir ağın daha derinlerine ilerlemeden önce, genellikle erişebilecekleri açık servisleri ve sistemleri tarar. Bu keşif adımı, bir sonraki aşamanın (yatay ilerleme ve daha fazla sızma) en güçlü habercisidir. Durumun erken safhada tespit edilmesi, güvenlik ekiplerine müdahale için kritik bir zaman penceresi kazandırıyor. Rapor, saldırı tekniklerini, gözlemlenen şüpheli faaliyetlerin ne kadarının kesinleşmiş

birer siber olaya dönüştüğüne bakarak sıralıyor. Kaspersky uzmanlarına göre, MITRE ATT&CK® matrisi çok geniş bir saldırgan tekniği kataloğu sunsa da etkili bir savunma için hatalı alarm üretmekten kaçınılmalı, kötü niyetli olma olasılığı en yüksek davranışlara öncelik verilmesi gerekiyor.

Kaspersky Güvenlik Operasyonları Merkezi (SOC) Müdürü Sergey Soldatov konuya ilişkin

şunları söylüyor: “Siber tehdit aktörleri hedeflerine ulaşmak için her zaman gelişmiş zararlı yazılımlara ihtiyaç duymazlar. Çoğu senaryoda, meşru yönetim araçları ve ele geçirilmiş hesaplar, fark edilmeden bir kurum içinde ilerlemenin en hızlı ve en etkili yoludur. Bu tekniklerin popülaritesini koruması; kurumların saldırgan davranışlarına karşı derin bir görünürlüğe ve bir saldırının farklı aşamalarındaki şüpheli faaliyetleri birbiriyle ilişkilendirme yeteneğine ihtiyaç duyduğunu gösteriyor. Şirketler bu zorlukların üstesinden gelmek için, tehdit tespitinden sürekli koruma ve müdahaleye kadar tüm olay yönetimi döngüsünü kapsayan Kaspersky Yönetilen Tespit ve Yanıt (MDR) ile Olay Müdahalesi (IR) çözümlerimizle güvenlik altyapılarını güçlendirebilirler.” Saldırgan taktik ve teknikleri, tespit edilen olayların nitelikleri, bunların bölgelere ve sektörlerle göre dağılımı hakkında daha fazla bilgi edinmek için raporun tamamını okuyabilirsiniz.

Yapay zekâ doktorunuz değil, danışırken dikkat edin

Siber güvenlik alanında dünya lideri olan ESET, tıbbi tavsiye almak için yapay zekâ kullanmanın güvenlik ve gizlilik risklerine maruz bırakabileceği uyarısında bulundu. Riskleri sıralayarak nasıl güvende kalınabileceğine yönelik önerilerini paylaştı.

ESET

Sohbet robotları düşünme, öğrenme ve çevremizdeki dünyayı algılama şeklimizi değiştiriyor. Bu tür bir dönüşüm hayatın birçok alanında kendini gösteriyor ancak belki de en hassas ve sıklıkla endişe verici olanlardan biri, sağlık hizmetleri için üretken yapay zekâ (GenAI) araçlarının giderek artan kullanımı. Siber güvenlik alanında dünya lideri olan ESET, tıbbi tavsiye almak için yapay zekâ kullanmanın güvenlik ve gizlilik risklerine maruz bırakabileceği uyarısında bulundu. Riskleri sıralayarak nasıl güvende kalınabileceğine yönelik önerilerini paylaştı. Bir dizi ücretsiz yapay zekâ sohbet robotunun yanı sıra büyük teknoloji şirketleri, kullanıcıların tıbbi kayıtlarını yorumlamalarına ve semptomları, laboratuvar sonuçları ve tedavi seçenekleri hakkında sorular sormalarına yardımcı olan Copilot Health, ChatGPT Health ve Amazon'un HealthAI gibi hizmetlerin lansmanıyla tüketicilere yönelik sağlık



yapay zekâ alanına girdi. Bir yapay zekâ aracının doktorun rolünü üstlenmesini beklemek bazı riskler barındırıyor. Risk sadece kullanıcıların yanlış tavsiye alması değil, aynı zamanda gizlilik korumaları, veri paylaşım uygulamaları ve yasal yükümlülükleri bir doktor veya hastaninkinden farklı olabilecek sistemlerle son derece hassas kişisel bilgileri paylaşmaları ve verilerinin beklenmedik kuruluşlara maruz kalmasıdır. Bir ABD hasta güvenliği kuruluşuna göre, genel olarak yapay zekâ sohbet robotlarının kötüye kullanımı şu

anda sağlık teknolojisi alanında bir numaralı tehlike konumunda. Microsoft'a göre, insanlar mobil cihazlarında diğer tüm konulardan daha fazla kendi sağlıkları ve sevdiklerinin sağlığı hakkında konuşuyor. Sohbet robotları 7/24 hizmet veriyor ve her şeye bir cevap sunarken gergin hastaları rahatlatmaya yardımcı olan kendinden emin bir üslupla konuşuyorlar. Ulusal sağlık sistemlerinin giderek daha fazla baskı altında olduğu bir dönemde, birçok kişi tıbbi yardım almaya karar vermeden önce muhtemelen yapay zekâ yardımıyla kendi kendine teşhis koyacak.

Ancak şimdiden bazı endişeler ortaya çıkmaya başladı. Bunlardan ilki, halüsinasyonlar veya yanlış tavsiyeler. Şubat ayında Nature Medicine dergisinde yayımlanan bir Oxford Üniversitesi araştırması şu bulguları ortaya koydu: Kullanıcılar genellikle LLM ile hangi bilgileri paylaşmaları gerektiğini bilmiyorlar; LLM'ler, kendilerine yöneltilen sorular çok az farklılık gösterse bile çok farklı cevaplar veriyor ve modeller genellikle hem iyi hem de kötü tavsiyelerde bulunuyor ancak kullanıcılar ikisini birbirinden ayırt etmekte zorlanıyor. Çalışmanın başhekimine göre tüm bu heyecana rağmen yapay zekâ henüz bir hekimin rolünü üstlenmeye hazır değil. Hastalar, semptomları hakkında büyük bir dil modeline danışmanın tehlikeli olabileceğini, yanlış teşhisler ortaya çıkabileceğini ve acil yardım gerektiğinde bunun farkına varılabileceğini bilmeli.

Yapay zekâ gizlilik riskleri

Bireylerin bir an durup düşüncelerini gerektirecek, sağlıkla ilgili olmayan riskler de bulunuyor. Hassas tıbbi bilgileri halka açık bir sohbet robotuyla paylaşmanın, verilerin modeli eğitmek için kullanılması ve dolayısıyla başkalarına aktarılması anlamına gelebileceği. Kasıtsız da olsa modellerin kullanıcıları tarafından girilen verileri yanlışlıkla ifşa ettiği biliniyor. Sağlık verileriniz, bilgileri değiştirilip yeniden düzenlenirken dondurulabilen çalıntı bir kredi kartı gibi değildir. Ömür boyu size aittir ve bir yapay zekâ aracıyla paylaşıldığında kalıcı bir dijital kayıt hâline gelebilir. Sağlık odaklı başlıca sohbet robotlarının çoğu,

bu verileri eğitim amaçlı kullanmayacaklarına dair söz veriyor. Eğitim gizlilik tablosunun sadece bir parçası ve hizmetler, üçüncü taraf veri paylaşımı konusunda aynı sözleri vermeyebilir. Kişisel tıbbi bilgileriniz, model sağlayıcısı ile sağlık hizmeti sağlayıcınız arasında yer alan bir üçüncü taraf olan veri toplayıcısının eline geçebilir. Ayrıca genellikle kullanımdan önce anonimleştirilse de doğrudan veya bu toplayıcılardan biri aracılığıyla reklam verenlerle paylaşılabilir. Sağlık verileri olağanüstü hassastır ve anonimleştirme her zaman tüm riskleri ortadan kaldırmaz.

İhlal riski katlandığında

Sağlık verileri, çeşitli nedenlerle dolandırıcılar tarafından yüksek oranda paraya çevrilebilir. Genellikle değiştirilemediği veya yeniden düzenlenemediği için uzun süre değerini korur. Sahte talepler sunmak veya sizin adınıza tıbbi hizmetler almak için kullanılabilecek sigorta bilgilerini içerebilir. Size şantaj yapmak için kullanılabilir. Bu verileri elinde bulunduran şirket sayısı ne kadar fazla olursa hackerların bu verileri ele geçirip çalma olasılığı da o kadar artar.

Yapay zekâ ile paylaştıklarınıza dikkat edin

Bir sağlık sorunu konusunda endişeleriniz varsa genel amaçlı botlardan uzak durun ve bunun yerine sağlıkla ilgili soruları yanıtlamak üzere özel olarak tasarlanmış botları tercih edin. Hizmetin verilerinizi nasıl işlediğini açıklayıp açıklamadığını, eğitim amacıyla girdiğiniz komutları

kullanıp kullanmadığını, bilgileri üçüncü taraflarla paylaşıp paylaşılmadığını ve bir gizlilik düzenlemesi kapsamında olup olmadığını kontrol edin. Doğrulamak için kaynak bağlantıları yoksa çıktıları körü körüne güvenmeyin. Cevapları mutlak gerçek olarak kabul etmeyin: Her zaman bir tıp uzmanına veya resmî bir web sitesine danışın.

Gizliliğinizi korumak için şunları göz önünde bulundurun:

- ▮ Araçların bu verileri nasıl işlediğini anlamadığınız sürece, tıbbi belgeleri, laboratuvar sonuçlarını veya diğer hassas belgeleri bir yapay zekâ aracıyla asla paylaşmayın, yüklemeyin.
 - ▮ İsim, adres, sigorta bilgileri, hasta numaraları veya diğer tanımlayıcı bilgileri girmekten kaçının.
 - ▮ Eğitim ve sohbet geçmişi özeliklerinin kapalı olduğundan emin olun.
 - ▮ Görev için gerekli olan minimum bilgiyi paylaşın.
 - ▮ Yazdığınız her şeyin saklanabileceğini veya ifşa edilebileceğini varsayın ve komutlarınızı buna göre ayarlayın.
- Yapay zekâ sohbet robotları, doktorunuza soracağınız belirli bir durumla ilgili soruları beyin fırtınası yapmak veya aşına olmadığınız bir tıbbi terimi açıklamak için yararlı olabilir. Ancak tıbbi bakım için hazırlık yapmak amacıyla yapay zekâ kullanmak ile tıbbi bakımın yerine yapay zekâyı kullanmak arasında büyük bir fark vardır. Kendinden emin bir cevabı tanı olarak kabul etmeyin ve bir makine sizi rahatlatığı için acil semptomları görmezden gelmeyin.

Açığa Çıkan IP Adresleri Dijital Kimlikleri Tehdit Ediyor

Bitdefender Türkiye Distribütörü Laykon Bilişim Operasyon Direktörü Alev Akkoyunlu, internet kullanıcılarını ve işletmeleri bu tehlikelere karşı uyararak dijital ayak izlerini koruyacak 5 hayati adımı aktarıyor.

LAYKON BİLİŞİM TEKNOLOJİLERİ



Global siber güvenlik lideri Bitdefender, dijital kimlik kartı sayılan IP adreslerinin ele geçirilmesinin, çevrimiçi izlenme ve doğrudan cihaz saldırıları gibi

risklerle mahremiyeti tehlikeye attığına dikkat çekiyor. Bitdefender Türkiye Distribütörü Laykon Bilişim Operasyon Direktörü Alev Akkoyunlu, internet kullanıcılarını ve işletmeleri bu tehlikelere karşı uyararak dijital ayak

izlerini koruyacak 5 hayati adımı aktarıyor. İnternete bağlanan her cihazın benzersiz bir kimliği olan IP adresi, dijital dünyada kullanıcıların nerede bulunduğunu ve hangi ağa bağlı olduğunu



ALEV AKKOYUNLU

gösteren temel bir bileşen işlevi görüyor. Bu adresin kötü niyetli kişilerin eline geçmesi, siber suçluların kullanıcıların fiziksel konumunu tahmin etmesine, ağa yönelik DDoS saldırıları düzenlemesine veya kişisel verileri hedef almasına olanak tanıyor. Özellikle şüpheli bağlantılara tıklamak veya güvensiz ağlara bağlanmak, IP adresinin kolayca açığa çıkmasına zemin hazırlıyor. Kontrolsüz bir şekilde bırakılan dijital ayak izleri kullanıcıların mahremiyetini tehlikeye atarken, Bitdefender Türkiye Distribütörü Laykon Bilişim Operasyon Direktörü Alev Akkoyunlu IP adresi güvenliğinin yol açtığı tehlikelere dikkat çekerek atılması gereken 5 adımı paylaşıyor.

“IP Adresinizi Korumadan Dijital Güvenliği Sağlayamazsınız”

İnternet üzerindeki her adımın bir iz bıraktığını belirten Laykon Bilişim Operasyon Direktörü Alev Akkoyunlu, “Kullanıcılar genellikle şifrelerini veya kredi kartı bilgilerini korumaya odak-

lansa da IP adresleri de en az bu veriler kadar kritik bir öneme sahip. Dijital ev adresiniz konumundaki bu bilginin açığa çıkması, ağınıza yönelik sızma girişimlerine veya çevrimiçi alışkanlıklarınızın izlenmesine yol açabiliyor. Cihazlarınızı ve ağınıza dışarıdan gelen tehditlere karşı korumanın en etkili yolu, bütünlük bir güvenlik stratejisi benimsemek ve çevrimiçi görünülüğünüzü minimuma indirmektir.” dedi.

Alev Akkoyunlu, kullanıcıların IP adreslerini gizlemek ve dijital mahremiyetlerini korumak için alması gereken 5 önlemi paylaşıyor:

1. Güvenilir bir sanal özel ağ (VPN) kullanın. VPN kullanmak, internet trafiğinizi şifreler ve gerçek IP adresinizi gizleyerek size farklı bir sunucu üzerinden yeni bir adres atar. Özellikle herkese açık ağlarda gezinirken VPN uygulamasını aktif tutmak, kimliğinizi siber korsanlardan saklamanın en güvenli yoludur.

2. Yönlendirici (Router) güvenliğinizi maksimuma çıkarın.

Ev veya iş ağınızın kalbi olan yönlendiricinizin varsayılan şifrelerini tahmin edilmesi zor kombinasyonlarla değiştirin. Aygıt yazılımını düzenli olarak güncelleyerek ağınıza dışarıdan yapılabilecek sızma girişimlerini engelleyin.

3. Şüpheli bağlantılara ve olta-lama mesajlarına karşı tetikte olun. Siber saldırganlar, IP adresinizi ele geçirmek için genellikle cazip görünen bağlantıları

“Global siber güvenlik lideri Bitdefender, dijital kimlik kartı sayılan IP adreslerinin ele geçirilmesinin, çevrimiçi izlenme ve doğrudan cihaz saldırıları gibi risklerle mahremiyeti tehlikeye attığına dikkat çekiyor.

veya sahte e-postalar gönderir. Kaynağını bilmediğiniz mesajlardaki bağlantılara tıklamaktan veya bilinmeyen dosyaları indirmekten kesinlikle kaçınin.

4. Gizlilik odaklı tarayıcılar ve arama motorları tercih edin. Siber saldırganlar genellikle eski yazılımlardaki açıkları kullanmayı tercih eder. Telefonunuzun işletim sistemini güncel tutarak siber korsanların faydalanabileceği güvenlik açıklarını kapatın.

5. Bütünlük güvenlik çözümleriyle cihazlarınızı koruma altına alın. Ağınıza yönelik olası saldırıları ve IP adresinizi hedef alan tehditleri anında durdurmak için cihazlarınızı Bitdefender Total Security gibi kapsamlı çözümlerle koruyarak arka planda tam güvenlik sağlayın.

Akıllı gözlükler **güvenlik riski taşıyor**

LAYKON BİLİŞİM TEKNOLOJİLERİ

İş dünyasında yapay zeka teknolojilerinin gelişmesiyle birlikte ortalama saldırıları boyut değiştirerek çok daha inandırıcı ve tehlikeli bir yapıya bürünüyor. Geleneksel yazılı e-postaların ötesine geçen siber saldırganlar, artık şirket CEO'larının veya üst düzey yöneticilerin seslerini saniyeler içinde kopyalayarak acil para transferi talep eden sahte sesli mesajlar veya video aramaları düzenliyor. Çalışanların üzerindeki otorite baskısını ve aciliyet duygusunu kullanan bu taktikler, milyonlarca liralık kayıplara yol açabiliyor. Çalışanların inisiyatifine bırakılan güvenlik süreçleri bu sofistike saldırılar karşısında yetersiz kalırken, Bitdefender Türkiye Distribütörü Laykon Bilişim Operasyon Direktörü Alev Akkoyunlu şirketlerin karşı karşıya kaldığı bu görünmez tehlikeye dikkat çekerek atılması gereken 4 adımı paylaşıyor.

“Yapay Zeka Destekli Taklitler Kurumsal Güvenliği Kökünden Sarsıyor”

Ses ve görüntü kopyalama teknolojilerinin siber suçluların elinde kusursuz bir silaha dönüştüğünü belirten Bitdefender Türkiye Distribütörü Laykon Bilişim Operasyon Direktörü Alev Akkoyunlu, “Çalışanlar, karşılarında bizzat şirket yöneticisinin sesini duyduklarında veya görüntüsünü gördüklerinde siber

güvenlik protokollerini kolayca göz ardı edebiliyor. Otorite figürlerinin bu derece inandırıcı bir şekilde taklit edilmesi, finans departmanlarını savunmasız bırakarak saniyeler içinde geri dönüşü olmayan fon kayıplarına neden oluyor. Kurumların bu yeni nesil tehditlerle başa çıkabilmesi, salt teknolojik önlemlerle sınırlı kalmayıp aynı zamanda çalışan farkındalığını en üst seviyeye çıkaran kapsamlı güvenlik kültürünün inşa edilmesine bağlıdır.” dedi. Alev Akkoyunlu, şirketlerin deepfake destekli patron dolandırıcılıklarına karşı alması gereken 4 önlemi paylaşıyor:

1. Finansal işlemler için katı ve çoklu onay protokolleri geliştirin. Büyük miktarda para transferleri veya hassas veri paylaşımları için asla tek bir iletişime güvenmeyin. E-posta, sesli arama veya video konferans yoluyla gelen acil ödeme taleplerini gerçekleştirmeden önce, işlemi farklı ve bağımsız iletişim kanalları üzerinden şirket içi onay mekanizmalarıyla mutlaka doğrulayın.

2. Şirket içi “güvenlik kelimeleri” veya gizli şifreler belirleyin. Yöneticiler ve kritik departman çalışanları arasında, acil durumlarda kimlik doğrulaması yapmak üzere önceden belirlenmiş ortak parolalar kullanın. Beklenmedik bir transfer talebi



geldiğinde bu şifrelerin sorulması, karşınızdaki kişinin yapay zeka destekli bir kopyadan ibaret olup olmadığını anlamının en pratik yollarından biridir.

3. Çalışanlarınızı yeni nesil yapay zeka tehditlerine karşı eğitin. Kurumsal siber güvenlik eğitimlerini, geleneksel ortalama (phishing) taktiklerinin ötesine taşıyın. Başta finans ve insan kaynakları olmak üzere tüm ekiplerinize deepfake teknolojisinin nasıl çalıştığını, sesli taklit saldırılarının belirtilerini ve şüpheli durumlar karşısında izlemeleri gereken adımları uygulamalı olarak gösterin.

4. Ağınızı ve cihazlarınızı kapsamlı bir çözümle koruma altına alın. Dolandırıcıların e-posta hesaplarınıza sızmasını veya deepfake araçlarını devreye sokmadan önce sisteminize zararlı yazılım yerleştirmesini engellemek için cihazlarınızı Bitdefender Total Security gibi kapsamlı çözümlerle koruyarak kurumunuzda tam güvenlik sağlayın.

Güvenlik Yönetimi

Ö Z E L G Ü V E N L İ K S E K T Ö R Ü N Ü N S E S İ

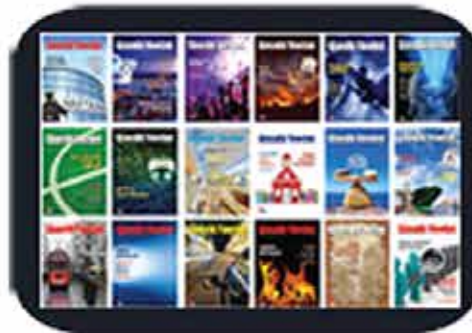


Özel Güvenlik Federasyonu'nun imtiyaz sahipliğini üstlendiği **Güvenlik Yönetimi Dergisi** havalimanları, Kamu Hastaneleri Birliği Genel Sekreterlikleri, AVM'ler, oteller, banka müdürlükleri, elektrik proje / taahhüt firmaları, inşaat şirketleri, TÜRK LİM (Türk Liman İşletmeleri) üyeleri, Emniyet Genel Müdürlükleri, Özel Güvenlik Daire Başkanlığı ve Özel Güvenlik Şube Müdürlükleri, bayi odaklı çalışan firmalara ve sektör profesyonellerine ulaşmaktadır. Gerek içeriği ve gerekse özel dağıtım ağıyla, sektörün nabzını tutan dergimiz, GÜSOD, GESİDER, ASIS ve ÖGF ile aynı platformda yer almaktadır.

Kapak, Fokus ve Özel Dosya konularımız başta olmak üzere, dergimizde sizin de projelerinize, teknik yazı ya da makalelerinize, ürün/sistem anlatımlarınıza ve reklamlarınıza yer vermek istiyoruz.



Turkcell Dergilik



www.guvenlikyonetimi.com



TurkTelecom E-dergi

Değişimi birlikte yakalayalım...



Katalog, Broşür Tasarımı	Logo Amblem Tasarım	Kurumsal Kimlik Tasarımı
Creative Çözümler	Baskı Çözümleri	Broşür ve Insert

arkhe
Tanıtım Hizmetleri

ARKHE TANITIM HİZMETLERİ
0542 250 72 49 - 0533 413 78 08
www.guvenlikyonetimi.com
www.guvenliktedarik.com

Güvenlik Yönetimi

ÖZEL GÜVENLİK SEKTÖRÜNÜN SESİ

E d i t ö r y e l T a k v i m

	KAPAK KONUSU	FOKUS KONUSU	ÖZEL DOSYA KONUSU
OCAK	Biyometrik Sistemler	Otel Güvenliği	Bina Otomasyon sistemleri
ŞUBAT	Para ve Kıymetli Eşya Taşıma	Spor Güvenliği	Drone Teknolojileri
MART	Yangın Algılama Sistemleri	AVM Güvenliği	VIP Koruma
NİSAN	Geçiş Kontrol Sistemleri	Endüstriyel Tesis Güvenliği	Toplumsal Davranış Psikolojisi ve Özel Güvenlik
MAYIS	CCTV ve Çevre Birimleri	Tarihi Varlıklar ve Müze Güvenliği	Acil Anos ve Seslendirme Sistemleri
HAZİRAN	Ulaşım Güvenliği	Tünel Uygulamaları	Hemşire Çağrı Sistemleri
TEMMUZ	Şehir izleme Sistemleri	Deniz ve Liman Güvenliği	Alarm İzleme Merkezleri
AĞUSTOS	Veri Yedekleme ve Depolama	Havalimanı Güvenliği	Dünyada ve Türkiye'de Özel Güvenlik
EYLÜL	Yangın Söndürme Sistemleri	Okul Öğrenci ve Kampüs Güvenliği	Duman Kontrol ve Tahliye Sistemleri
EKİM	Bilgi Güvenliği	Hastane Güvenliği	Güvenlikte Kablo
KASIM	Araç Takip Sistemleri	Kritik Tesis Güvenliği	Çevre Güvenliği
ARALIK	Sektöre Yön Verenler	Mağaza Güvenliği	Afet ve Tahliye Güvenliği

R E K L A M İ N D E K İ



19



65



15



23



9



5



11



13



AK



17



45



70



9

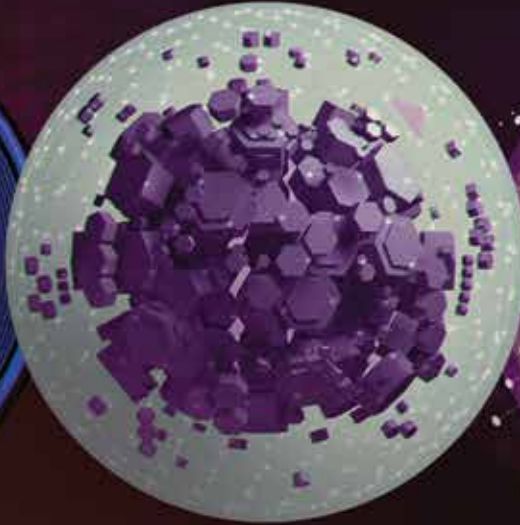


Western Digital.

GÜVENLİK GÖZETİMİNDEN ÖTE



YAKALAYIN



DEPOLAYIN



ANALİZ EDİN



Western Digital, Western Digital logosu, WD, WD Logosu, Ultrastar ve WD Purple, Western Digital Corporation şirketinin veya iştiraklerinin ABD ve/veya diğer ülkelerdeki tescilli ticari markaları ya da ticari markalarıdır. microSD işareti ve logosu, SD-3C, LLC'nin ticari markalarıdır. Diğer tüm markalar, ilgili sahiplerin mülkiyetindedir. Performans, donanım ve yazılım bileşenleriniz ile yapılandırılmalarına bağlı olarak değişir. Ürün özellikleri uyarında bulunulmaksızın değiştirilebilir. Görülen resimler asıl ürünlerden farklı olabilir.

©2018 Western Digital Corporation veya iştirakleri. Tüm hakları saklıdır.